

**EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA**

**YADY MILENA VILLAMIL MONTES**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA, ECBTI  
PROGRAMA DE INGENIERIA DE SISTEMAS  
CEAD: VELEZ  
2019**

# **EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA**

**YADY MILENA VILLAMIL MONTES**

**Informe**

**Tutor**

**Gerardo Granados Acuña**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA, ECBTI  
PROGRAMA DE INGENIERIA DE SISTEMAS  
CEAD: VELEZ  
2019**

## **AGRADECIMIENTOS**

Agradezco primeramente a Dios por permitirme la vida para llegar a donde estoy, porque siempre bendice mi vida con grandes oportunidades, a mis padres por ser mi motor para cumplir mis sueños, por cada día confiar y creer en mí, por darme la oportunidad de estudiar la carrera de Ingeniería para superarme y ser alguien en la vida, por todos los consejos que me han brindado para no rendirme en los momentos difíciles, por ayudarme a tomar las mejores decisiones que me ayudan a crecer como persona.

Agradezco a los tutores que con sus explicaciones y respuestas a cada una de mis inquietudes durante el desarrollo de este informe y del curso en general, contribuyeron para poder adquirir conocimientos que serán de apoyo en mi vida laboral y profesional.

## CONTENIDO

pág

<b>GLOSARIO .....</b>	<b>8</b>
<b>RESUMEN .....</b>	<b>10</b>
<b>INTRODUCCIÓN .....</b>	<b>11</b>
<b>1. ESCENARIO 1 .....</b>	<b>12</b>
<b>2. ESCENARIO 2 .....</b>	<b>48</b>
<b>CONCLUSIÓN.....</b>	<b>72</b>
<b>BIBLIOGRAFÍA.....</b>	<b>73</b>

## LISTA DE TABLAS

	pág
Tabla 1. Direccionamiento escenario 1.....	13
Tabla 2. Direccionamiento escenario 2.....	48
Tabla 3. OSPFv2 area 0.....	57
Tabla 4. Configurar DHCP pool.....	67

## LISTA DE FIGURAS

	pág
Figura 1. Topología de red escenario 1.....	12
Figura 2. IP estática de las PC.....	24
Figura 3. Ping del router Bogotá 1.....	24
Figura 4. Ping del router Bogotá 2.....	25
Figura 5. Ping del router Bogotá 3.....	25
Figura 6. Ping del router Medellín 1.....	26
Figura 7. Ping del router Medellín 2.....	26
Figura 8. Ping del router Medellín 3.....	27
Figura 9. Ping de las PC a los router.....	27
Figura 10. Red principal de Bogotá y Medellín.....	31
Figura 11. Ping de Medellín 1.....	32
Figura 12. Ping de Bogotá 1.....	33
Figura 13. Verificar tabla de enrutamiento en los router.....	33
Figura 14. Comando show run para Bogotá 1.....	34
Figura 15. Comando show run para Bogotá 2.....	35
Figura 16. Comando show run para Medellín 1.....	36
Figura 17. Comando show run para Medellín 2.....	37
Figura 18. Comando show run para ISP.....	38
Figura 19. Verificar la base de datos de RIP.....	40
Figura 20. Ping de Medellín 1 al ISP.....	41

Figura 21. Ping de Bogotá 1 al ISP.....	42
Figura 22. DHCP en los PC de Medellín.....	43
Figura 23. DHCP en los PC de Bogotá.....	44
Figura 24. Verificar IP con el comando ipconfig.....	45
Figura 25. Ping de PC-150 a los demás PC.....	45
Figura 26. Verificar con ping conectividad.....	47
Figura 27. Topología de red escenario 2.....	48
Figura 28. Dirección IP de Internet PC y Web Server.....	55
Figura 29. Ping de Bogotá a Miami.....	55
Figura 30. Ping de Buenos Aires a Miami.....	55
Figura 31. Ping de Miami a Bogotá y Buenos Aires.....	56
Figura 32. Ping del Miami a Internet PC y Web Server.....	56
Figura 33. Ping de Internet PC a Miami.....	56
Figura 34. Ping de Web Server a Miami.....	56
Figura 35. Visualizar tablas de enrutamiento y router conectados por OSPFv2.....	59
Figura 36. Visualizar lista resumida de interfaces por OSPF.....	59
Figura 37. Visualizar el OSPF, process ID, router ID, address, summarization, routing networks, and passive interfaces configuradas en cada router.....	60
Figura 38. DHCP en los PC.....	69
Figura 39. Ping de PC-A a PC-C, Internet PC y Web Server.....	69
Figura 40. Ping de PC-C a PC-A, Internet PC y Web Server.....	70
Figura 41. Telnet para entrar al router.....	70

## GLOSARIO

**CONECTIVIDAD:** Es la capacidad de un dispositivo de poder ser conectado, por lo general a una computadora personal u otro dispositivo electrónico, sin la necesidad de un ordenador, es decir en forma autónoma.

**ENCAPSULAMIENTO:** Es un mecanismo que consiste en organizar datos y métodos de una estructura, conciliando el modo en que el objeto se implementa, es decir, evitando el acceso a datos por cualquier otro medio distinto a los especificados. Por lo tanto, la encapsulación garantiza la integridad de los datos que contiene un objeto.

**RED:** Nombra al conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios.

**ROUTER:** Es un dispositivo de red que se encarga de llevar por la ruta adecuada el tráfico. Funcionan utilizando direcciones IP para saber a donde tienen que ir los paquetes de datos.

**SWITCH:** Es un dispositivo que sirve para conectar varios elementos dentro de una red.

**AUTENTICACIÓN:** Es el acto o proceso de confirmar que algo (o alguien) es quien dice ser.

**ENRUTAMIENTO:** Es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda.

**PROTOCOLO RIP:** Es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

**RUTA ESTÁTICA:** Generalmente se establece en el router, aunque también se puede configurar localmente desde el símbolo del sistema de Windows.

**SHOW RUN:** Este comando imprime en pantalla la configuración actual del router.

**INTERFAZ PASIVA:** Se utiliza para suprimir tráfico de actualización innecesario, por ejemplo, cuando una interfaz es una interfaz LAN, sin otros routers conectados.



**AUTENTICACIÓN PAP:** Es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet.

**AUTENTICACIÓN CHAP:** Es un método de autenticación remota o inalámbrica. Diversos proveedores de servicios emplean CHAP. Por ejemplo, para autenticar a un usuario frente a un ISP.

**SERVIDOR DHCP:** Es el protocolo de configuración dinámica de host, un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica a los clientes DHCP de la red, de direcciones IP y de otros detalles de configuración relacionados con el direccionamiento IP.

## RESUMEN

El trabajo se desarrollará con el fin de presentar la solución de la prueba de habilidades prácticas del curso de profundización de CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), mediante las cuales se colocan a la vista las temáticas desarrolladas durante todo el curso, los conocimientos adquiridos y aplicados en temas de redes Cisco.

Se desarrollarán 2 escenarios para dar a conocer lo aprendido en el diplomado de profundización cisco, detallando los pasos y comandos utilizados para su correcto desarrollo, también se mostrará las respectivas imágenes para verificar la conectividad de toda la red.

En el escenario uno se dará a conocer, como configurar el enrutamiento de red usando el protocolo RIP versión 2 para redistribuirlo en las publicaciones RIP, las rutas estáticas dirigidas hacia cada red interna, aprender a deshabilitar la propagación RIP, realizar su respectiva verificación, encapsulamiento y autenticación PPP, configurar PAT y servicio DHCP.

En el escenario dos se mostrará como configurar el direccionamiento IP acorde a la topología propuesta, configurar el protocolo de enrutamiento OSPFv2, verificar su respectiva información, configuración de VLANs, puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y seguridad en los switches acorde a la topología de red establecida, implementar DHCP y NAT para IPv4.

Es importante destacar el grado de importancia que tiene el simulador Cisco Packet Tracer, ya que, sin la ejecución del mismo, la interpretación y grado de análisis serían nulos, es importante tener en cuenta que la visión que ofrece nos permite adquirir conocimiento y desarrollar si se quiere la crítica necesaria para inferir en decisiones de implementación y diseño en una red.

## INTRODUCCIÓN

En el informe se ha perfeccionado las habilidades aprendidas durante el curso, el aprendizaje ha estado enfocado a la configuración de los SWITCHES, ROUTER así como también las características de seguridad de los mismos, la configuración de IPv4, la creación y configuración de VLANS, puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN, Routing, implementar DHCP y NAT para IPv4, por otro lado, configurar el enrutamiento de red usando el protocolo RIP versión 2 para redistribuirlo en las publicaciones RIP, las rutas estáticas dirigidas hacia cada red interna, deshabilitar la propagación RIP, encapsulamiento y autenticación PPP y configurar PAT.

Las necesidades de red en el entorno hacen que todas las experiencias de aprendizaje logradas con el desarrollo del trabajo, puedan ser de ayuda en los casos que se deben enfrentar a diario.

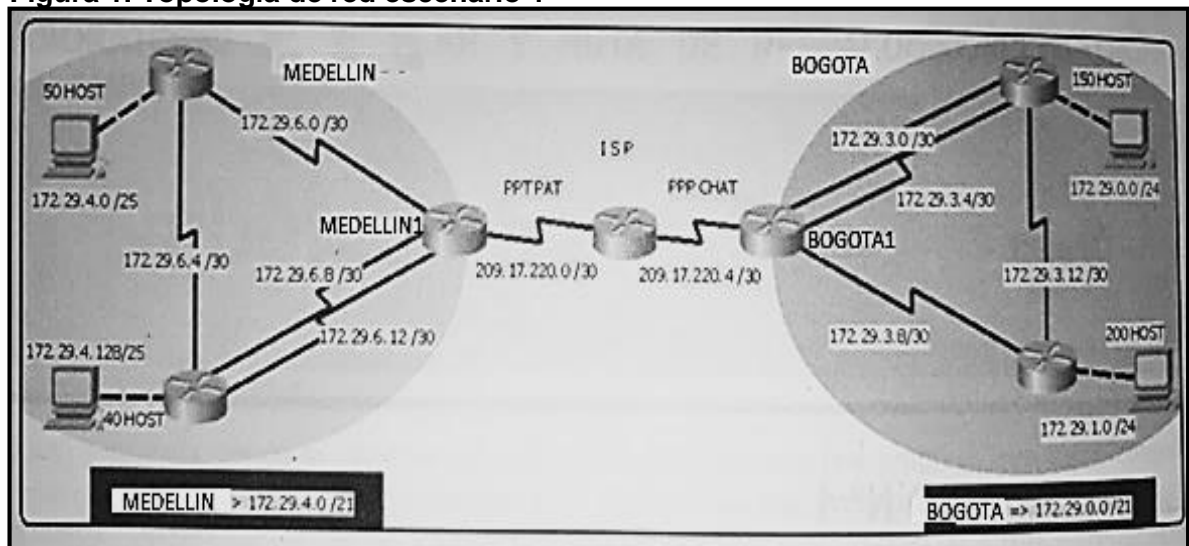
Se tendrá dos escenarios que se deben desarrollar mediante el uso de la herramienta de Simulación PACKET TRACER, que es la herramienta de aprendizaje y simulación de redes interactiva para instructores y alumnos de Cisco. Esta herramienta permite crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

Una de las grandes ventajas de utilizar este programa es que permite ver cómo deambulan los paquetes por los diferentes equipos, además de poder analizar de forma rápida el contenido de cada uno de ellos en las diferentes capas.

## 1. ESCENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

**Figura 1. Topología de red escenario 1**



Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

**Tabla 1. Direccionamiento escenario 1**

<b>Dispositivo</b>	<b>Interfaz</b>	<b>Dirección IP</b>	<b>Mascara de subred</b>	<b>Gateway predeterminado</b>
Bogotá 1	S0/0/1	172.29.3.1	255.255.255.252	N/A
	S0/1/0	172.29.3.5	255.255.255.252	N/A
	S0/1/1	172.29.3.9	255.255.255.252	N/A
	S0/0/0	209.17.220.5	255.255.255.252	N/A
Bogotá 2	S0/0/0	172.29.3.10	255.255.255.252	N/A
	S0/0/1	172.29.3.13	255.255.255.252	N/A
	G0/0	172.29.1.1	255.255.255.0	N/A
Bogotá 3	S0/0/0	172.29.3.2	255.255.255.252	N/A
	S0/0/1	172.29.3.6	255.255.255.252	N/A
	S0/1/0	172.29.3.14	255.255.255.252	N/A
	G0/0	172.29.0.1	255.255.255.0	N/A
Medellín 1	S0/0/0	172.29.6.1	255.255.255.252	N/A
	S0/0/1	172.29.6.13	255.255.255.252	N/A
	S0/1/1	172.29.6.9	255.255.255.252	N/A
	S0/1/0	209.17.220.1	255.255.255.252	N/A
Medellín 2	S0/0/0	172.29.6.5	255.255.255.252	N/A
	S0/0/1	172.29.6.2	255.255.255.252	N/A
	G0/0	172.29.4.1	255.255.255.128	N/A
Medellín 3	S0/0/0	172.29.6.10	255.255.255.252	N/A
	S0/0/1	172.29.6.14	255.255.255.252	N/A
	S0/1/0	172.29.6.6	255.255.255.252	N/A
	G0/0	172.29.4.129	255.255.255.128	N/A
ISP	S0/0/1	209.17.220.6	255.255.255.252	N/A
	S0/0/0	209.17.220.2	255.255.255.252	N/A
PC-150 host	NIC	DHCP	DHCP	DHCP
PC-200 host	NIC	DHCP	DHCP	DHCP
PC-50 host	NIC	DHCP	DHCP	DHCP
PC-40 host	NIC	DHCP	DHCP	DHCP

## **DESARROLLO**

1. Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

### **Router Bogotá 1**

Press RETURN to get started!

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota1
Bogota1(config)#no ip domain-lookup
Bogota1(config)#enable password class
Bogota1(config)#line con 0
Bogota1(config-line)#password cisco
Bogota1(config-line)#login
Bogota1(config-line)#exit
Bogota1(config)#line vty 0 15
Bogota1(config-line)#password cisco
Bogota1(config-line)#login
Bogota1(config-line)#exit
Bogota1(config)#service password-encryption
Bogota1(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Bogota1(config)#end
Bogota1#
%SYS-5-CONFIG_: Configured from console by console
Bogota1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota1#

```

## **Router Bogotá 2**

Press RETURN to get started!

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota2
Bogota2(config)#no ip domain-lookup
Bogota2(config)#enable password class
Bogota2(config)#line con 0
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit
Bogota2(config)#line vty 0 15
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit

```

```
Bogota2(config)#service password-encryption
Bogota2(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Bogota2(config)#end
Bogota2#
%SYS-5-CONFIG_I: Configured from console by console
Bogota2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota2#
```

### **Router Bogotá 3**

Press RETURN to get started!

```
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota3
Bogota3(config)#no ip domain-lookup
Bogota3(config)#enable password class
Bogota3(config)#line con 0
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#exit
Bogota3(config)#line vty 0 15
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#exit
Bogota3(config)#service password-encryption
Bogota3(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Bogota3(config)#end
Bogota3#
%SYS-5-CONFIG_I: Configured from console by console
Bogota3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota3#
```

### **Router Medellín 1**

Press RETURN to get started!

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin1
Medellin1(config)#no ip domain-lookup
Medellin1(config)#enable password class
Medellin1(config)#line con 0
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#exit
Medellin1(config)#line vty 0 15
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#exit
Medellin1(config)#service password-encryption
Medellin1(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Medellin1(config)#end
Medellin1#
%SYS-5-CONFIG_: Configured from console by console
Medellin1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Medellin1#

```

## **Router Medellín 2**

Press RETURN to get started!

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin2
Medellin2(config)#no ip domain-lookup
Medellin2(config)#enable password class
Medellin2(config)#line con 0
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#exit
Medellin2(config)#line vty 0 15
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#exit
Medellin2(config)#service password-encryption

```



```
Medellin2(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Medellin2(config)#end
Medellin2#
%SYS-5-CONFIG_I: Configured from console by console
Medellin2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Medellin2#
```

### **Router Medellín 3**

Press RETURN to get started!

```
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin3
Medellin3(config)#no ip domain-lookup
Medellin3(config)#enable password class
Medellin3(config)#line con 0
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#exit
Medellin3(config)#line vty 0 15
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#exit
Medellin3(config)#service password-encryption
Medellin3(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Medellin3(config)#end
Medellin3#
%SYS-5-CONFIG_I: Configured from console by console
Medellin3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Medellin3#
```

### **Router ISP**

```
Router>enable
Router#configure t
```

```

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#enable password class
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd "Prohibido el ingreso a personal no autorizado"
ISP(config)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console
ISP#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#

```

2. Realizar la conexión física de los equipos con base en la topología de red

### **Router Bogotá 1**

Password:

```

Bogota1>enable
Password:
Bogota1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#interface s0/0/1
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Bogota1(config-if)#interface s0/1/0
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Bogota1(config-if)#interface s0/1/1
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252

```

```

Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Bogota1(config-if)#interface s0/0/0
Bogota1(config-if)#ip address 209.17.220.5 255.255.255.252
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Bogota1(config-if)#end
Bogota1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota1#

```

## Router Bogotá 2

Prohibido el ingreso a personal no autorizado

```

User Access Verification
Password:
Bogota2>enable
Password:
Bogota2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#interface s0/0/0
Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota2(config-if)#no shutdown
Bogota2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Bogota2(config-if)#interface s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Bogota2(config-if)#interface g0/0
Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shutdown
Bogota2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Bogota2(config-if)#exit
Bogota2(config)#exit
Bogota2#copy run start

```

Destination filename [startup-config]?  
Building configuration...  
[OK]  
Bogota2#

### **Router Bogotá 3**

Password:  
Bogota3>enable  
Password:  
Bogota3#configure t  
Enter configuration commands, one per line. End with CNTL/Z.  
Bogota3(config)#interface s0/0/0  
Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252  
Bogota3(config-if)#no shutdown  
Bogota3(config-if)#  
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up  
Bogota3(config-if)#interface s0/0/1  
Bogota3(config-if)#ip address 172.29.3.6 255.255.255.252  
Bogota3(config-if)#no shutdown  
Bogota3(config-if)#  
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up  
Bogota3(config-if)# interface s0/1/0  
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252  
Bogota3(config-if)#no shutdown  
Bogota3(config-if)#  
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up  
Bogota3(config-if)#interface g0/0  
Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0  
Bogota3(config-if)#no shutdown  
Bogota3(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,  
changed state to up  
Bogota3(config-if)#end  
Bogota3#copy run start  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
Bogota3#

### **Router Medellín 1**

Password:

Medellin1>enable

Password:

Medellin1#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Medellin1(config)#interface s0/0/0

Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252

Medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Medellin1(config-if)#interface s0/0/1

Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252

Medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Medellin1(config-if)#interface s0/1/1

Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252

Medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down

Medellin1(config-if)#interface s0/1/0

Medellin1(config-if)#ip address 209.17.220.1 255.255.255.252

Medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down

Medellin1(config-if)#end

Medellin1#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

Medellin1#

## **Router Medellín 2**

Password:

Medellin2>enable

Password:

Medellin2#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Medellin2(config)#interface s0/0/0

Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252

Medellin2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Medellin2(config-if)#interface s0/0/1

Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252

Medellin2(config-if)# no shutdown

```
Medellin2(config-if)#interface g0/0
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown
Medellin2(config-if)#end
Medellin2#
%SYS-5-CONFIG_I: Configured from console by console
Medellin2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Medellin2#
```

### **Router Medellín 3**

Password:

```
Medellin3>enable
Password:
Medellin3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#interface s0/0/0
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Medellin3(config-if)#interface s0/0/1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Medellin3(config-if)#interface s0/1/0
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
Medellin3(config-if)#interface g0/0
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Medellin3(config-if)#end
```

```
Medellin3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Medellin3#
```

## **Router ISP**

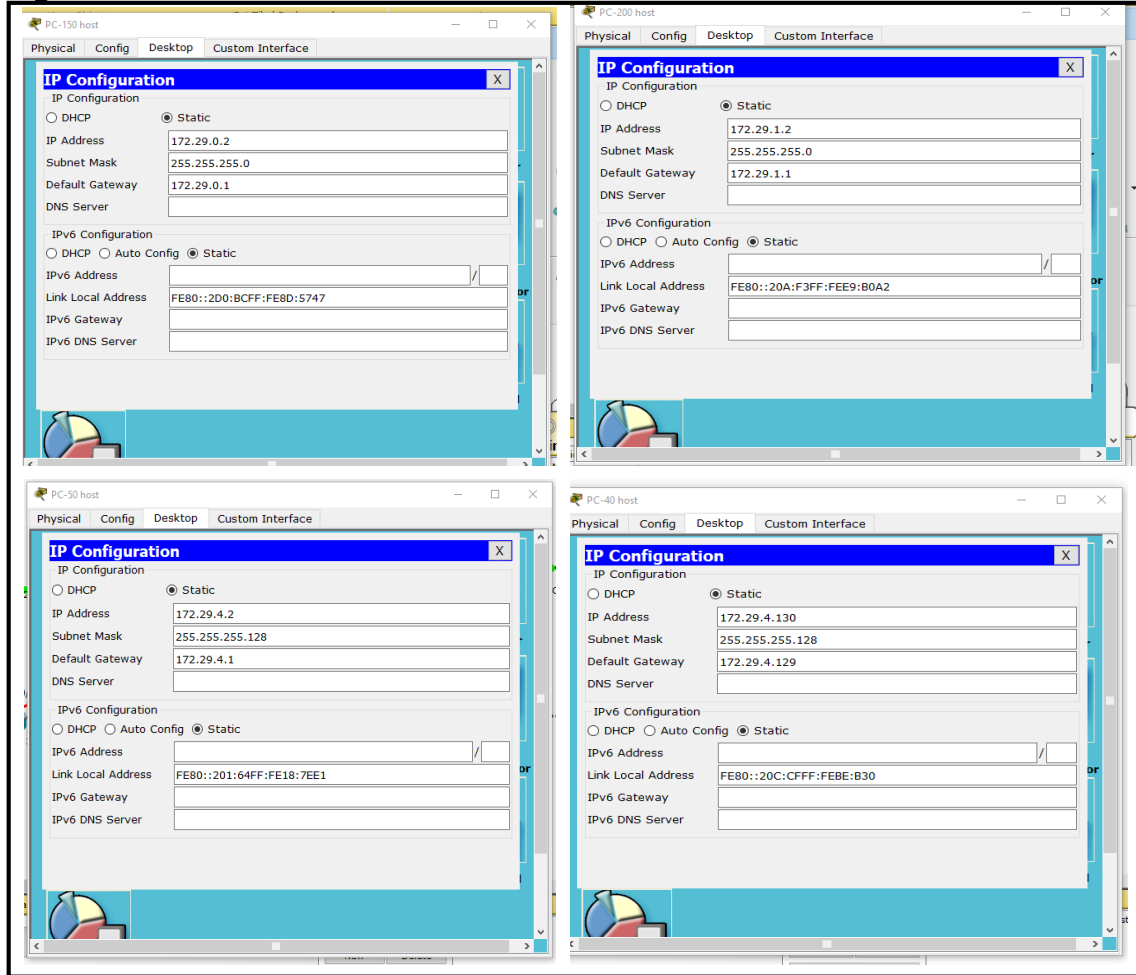
User Access Verification

Password:

```
ISP>enable
Password:
ISP#configure t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface s0/0/0
ISP(config-if)#ip address 209.17.220.2 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ISP(config-if)#interface s0/0/1
ISP(config-if)#ip address 209.17.220.6 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
ISP(config-if)#end
ISP#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

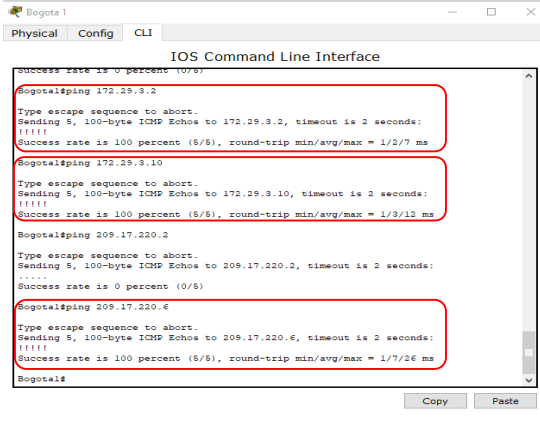
IP estática de las PC, mientras se configura el DHCP

**Figura 2. IP estática de las PC**



Ping del router Bogotá 1 al router Bogotá 2, Bogotá 3 y el router ISP

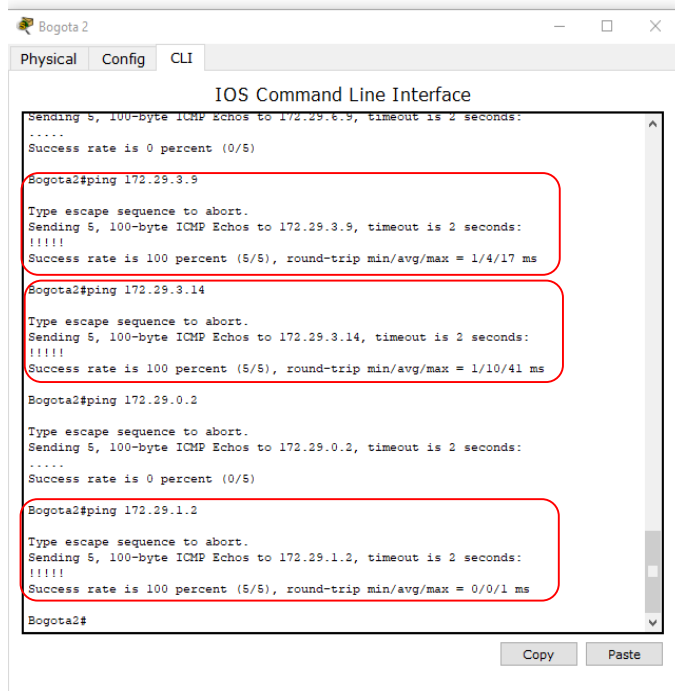
**Figura 3. Ping del Router Bogota1**





Ping del router Bogota 2 al router Bogotá 1, Bogotá 3 y a la PC-200 host

**Figura 4. Ping del Router Bogota2**



```
Bogota2
Physical Config CLI
IOS Command Line Interface

Sending 5, 100-byte ICMP Echos to 172.29.3.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Bogota2#ping 172.29.3.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.9, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms

Bogota2#ping 172.29.3.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.14, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/41 ms

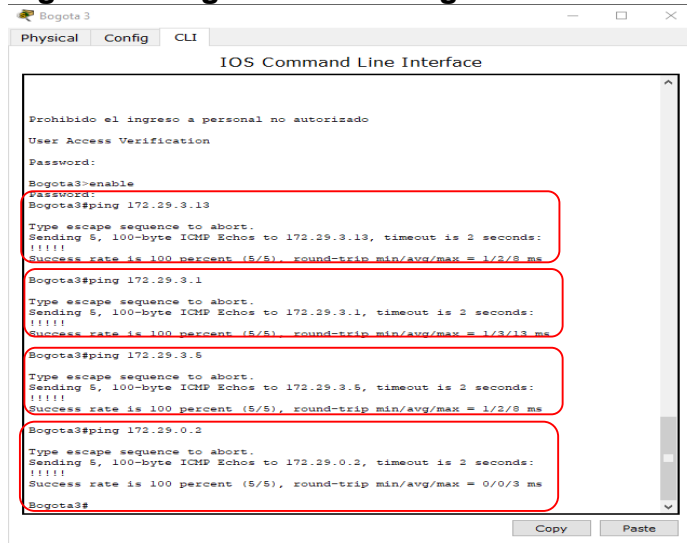
Bogota2#ping 172.29.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Bogota2#ping 172.29.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Bogota2#
```

Ping del router Bogota 3 al router Bogotá 1 con los dos seriales, Bogotá 2 y a la PC-150 host

**Figura 5. Ping del Router Bogota3**



```
Bogota3
Physical Config CLI
IOS Command Line Interface

Prohibido el ingreso a personal no autorizado
User Access Verification
Password:
Bogota3>enable
Password:
Bogota3#ping 172.29.3.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.13, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Bogota3#ping 172.29.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/13 ms

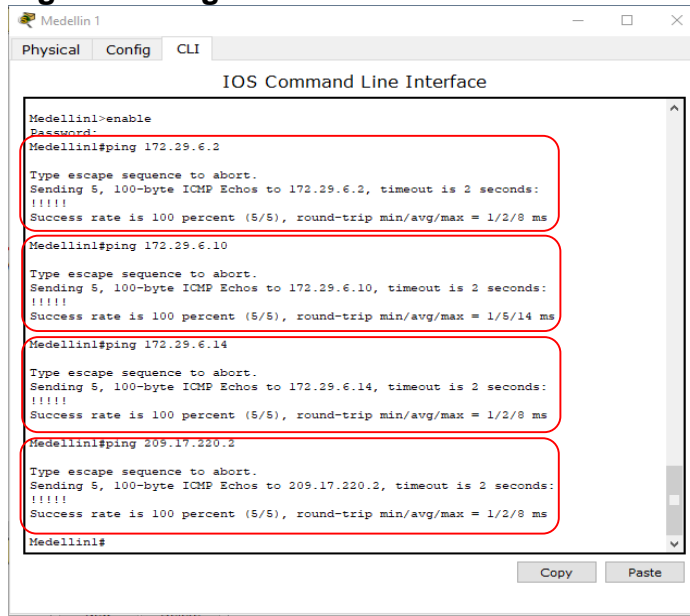
Bogota3#ping 172.29.3.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Bogota3#ping 172.29.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.0.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

Bogota3#
```

Ping del router Medellín 1 al router Medellín 2 , Medellín 3 y el router ISP

**Figura 6. Ping del Router Medellin1**



```
Medellin1>enable
Password:
Medellin1#ping 172.29.6.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Medellin1#ping 172.29.6.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/14 ms

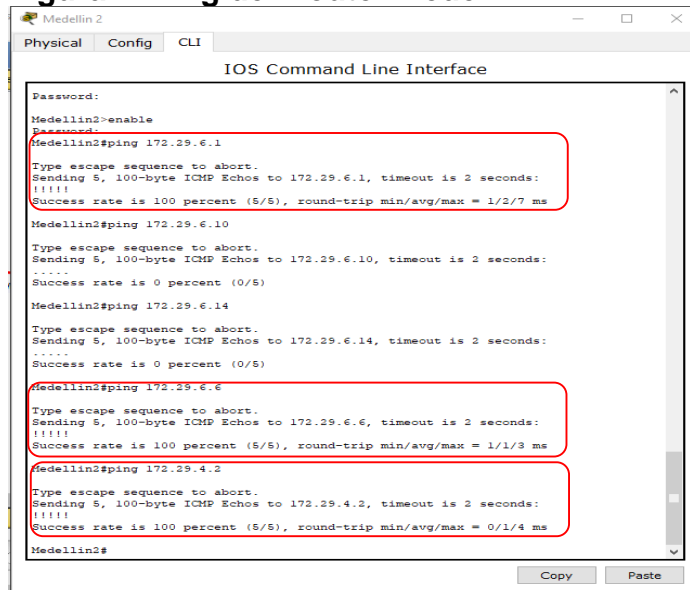
Medellin1#ping 172.29.6.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.14, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Medellin1#ping 209.17.220.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Medellin1#
```

Ping del router Medellín 2 al router Medellín 1 , Medellín 3 y el PC-50 host

**Figura 7. Ping del Router Medellin2**



```
Medellin2>enable
Password:
Medellin2#ping 172.29.6.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms

Medellin2#ping 172.29.6.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Medellin2#ping 172.29.6.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Medellin2#ping 172.29.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

Medellin2#ping 172.29.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

Medellin2#
```

Ping del router Medellín 3 al router Medellín 1 , Medellín 2 y el PC-40 host

**Figura 8. Ping del Router Medellin3**

```

Medellin3
Physical Config CLI
IOS Command Line Interface

Password:
Medellin3>enable
Password:
Medellin3#ping 172.29.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Medellin3#ping 172.29.6.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.13, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

Medellin3#ping 172.29.6.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.9, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/49 ms

Medellin3#ping 172.29.6.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.5, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms

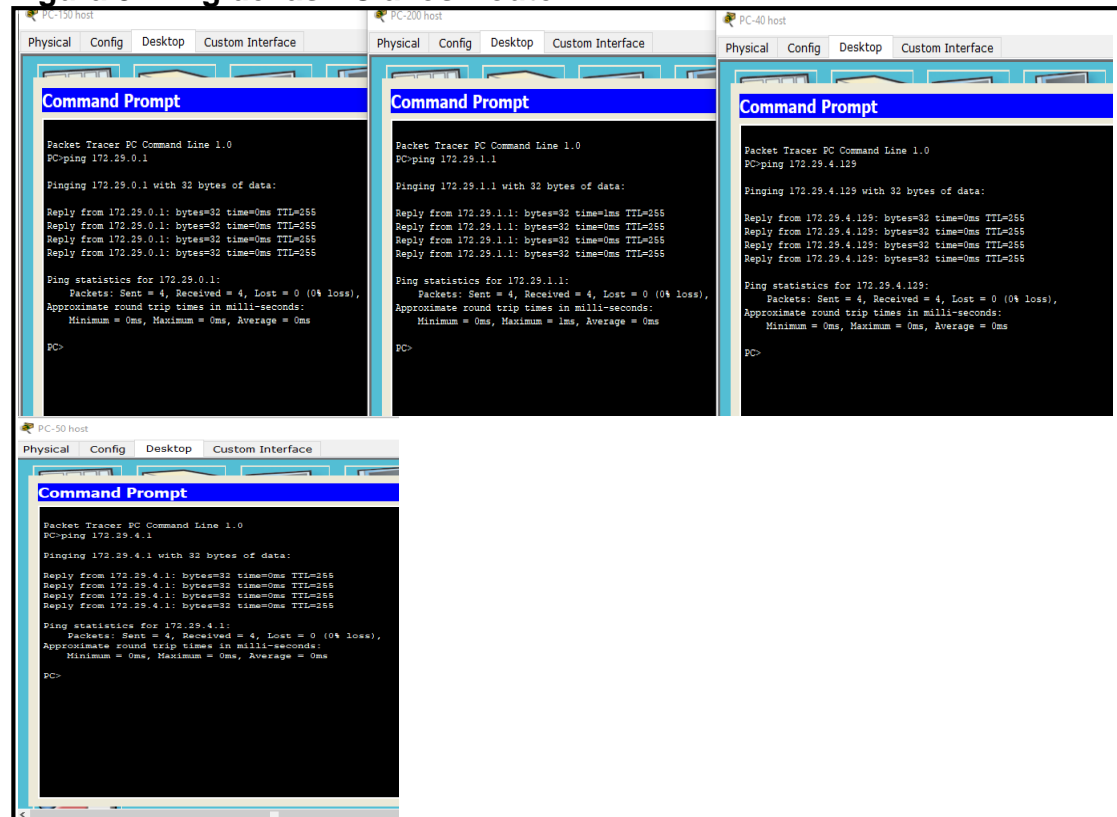
Medellin3#ping 172.29.4.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.4.130, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

Medellin3#
Copy Paste
  
```

Ping de las PC a sus respectivos router

**Figura 9. Ping de las PC a los Router**



3. Configurar el enrutamiento en la red usando el protocolo RIP versión 2, declare la red principal, desactive la sumarización automática.

### **Router Medellín 1**

```
Password:
Medellin1>enable
Password:
Medellin1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#router rip
Medellin1(config-router)#version 2
Medellin1(config-router)#no auto-summary
Medellin1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/1/1
C 172.29.6.12/30 is directly connected, Serial0/0/1
C 209.17.220.0/30 is directly connected, Serial0/1/0
Medellin1(config-router)#network 172.29.6.0
Medellin1(config-router)#network 172.29.6.8
Medellin1(config-router)#network 172.29.6.12
Medellin1(config-router)#
```

### **Router Medellín 2**

```
Medellin2>enable
Password:
Medellin2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#router rip
Medellin2(config-router)#version 2
Medellin2(config-router)#no auto-summary
Medellin2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.4/30 is directly connected, Serial0/0/0
Medellin2(config-router)#network 172.29.4.0
Medellin2(config-router)#network 172.29.6.0
Medellin2(config-router)#network 172.29.6.4
Medellin2(config-router)#
```

### **Router Medellín 3**

```
Medellin3>enable
Password:
Medellin3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#router rip
Medellin3(config-router)#version 2
Medellin3(config-router)#no auto-summary
Medellin3(config-router)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/0/1
Medellin3(config-router)#network 172.29.4.128
Medellin3(config-router)#network 172.29.6.4
Medellin3(config-router)#network 172.29.6.8
Medellin3(config-router)#network 172.29.6.12
Medellin3(config-router)#
```

### **Router Bogotá 1**

```
Bogota1>enable
Password:
Bogota1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#router rip
Bogota1(config-router)#version 2
Bogota1(config-router)#no auto-summary
Bogota1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/0
C 172.29.3.8/30 is directly connected, Serial0/1/1
C 209.17.220.4/30 is directly connected, Serial0/0/0
Bogota1(config-router)#network 172.29.3.0
Bogota1(config-router)#network 172.29.3.4
Bogota1(config-router)#network 172.29.3.8
Bogota1(config-router)#
```

### **Router Bogotá 2**

```
Password:
Bogota2>enable
Password:
Bogota2#configure t
```

Enter configuration commands, one per line. End with CNTL/Z.

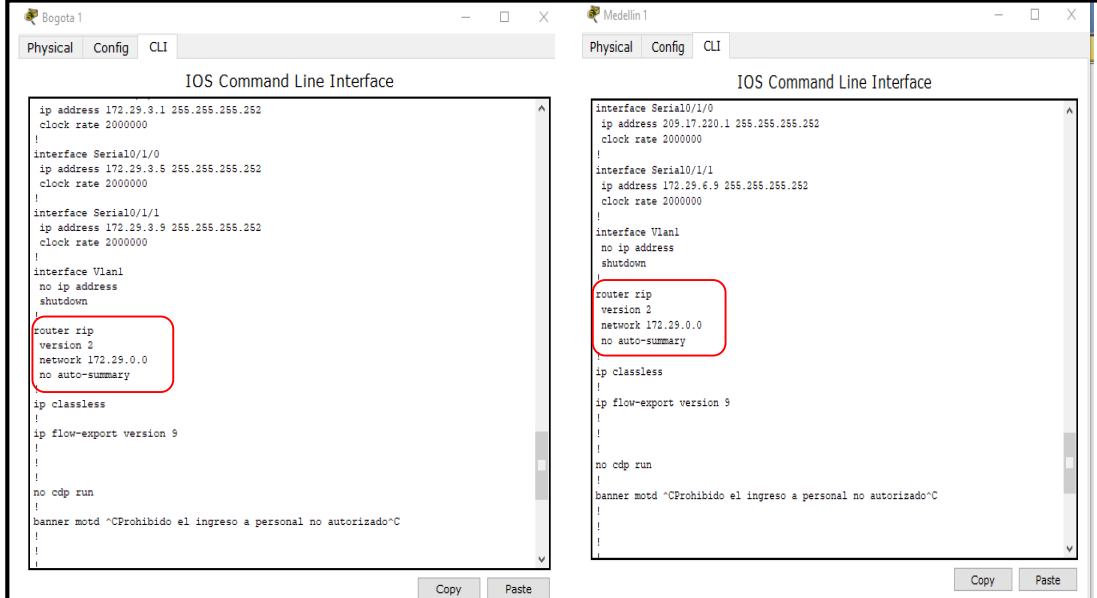
```
Bogota2(config)#router rip
Bogota2(config-router)#version 2
Bogota2(config-router)#no auto-summary
Bogota2(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
Bogota2(config-router)#network 172.29.1.0
Bogota2(config-router)#network 172.29.3.8
Bogota2(config-router)#network 172.29.3.12
Bogota2(config-router)#
```

### **Router Bogotá 3**

```
Bogota3>enable
Password:
Bogota3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#router rip
Bogota3(config-router)#version 2
Bogota3(config-router)#no auto-summary
Bogota3(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0
Bogota3(config-router)#network 172.29.0.0
Bogota3(config-router)#network 172.29.3.0
Bogota3(config-router)#network 172.29.3.4
Bogota3(config-router)#network 172.29.3.12
Bogota3(config-router)#
```

La red principal en Bogota 1 y Medellin 1 es network 172.29.0.0

**Figura 10. Red principal de Bogotá y Medellín**



4. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de RIP.

### Router Medellín 1

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

Medellin1>enable

Password:

Medellin1#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2

Medellin1(config)#router rip

Medellin1(config-router)#default-information originate

Medellin1(config-router)#

### Router Bogotá 1

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

```

Bogota1>enable
Password:
Bogota1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.6
Bogota1(config)#router rip
Bogota1(config-router)#default-information originate
Bogota1(config-router)#

```

5. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se suman las subredes de cada uno a /22.

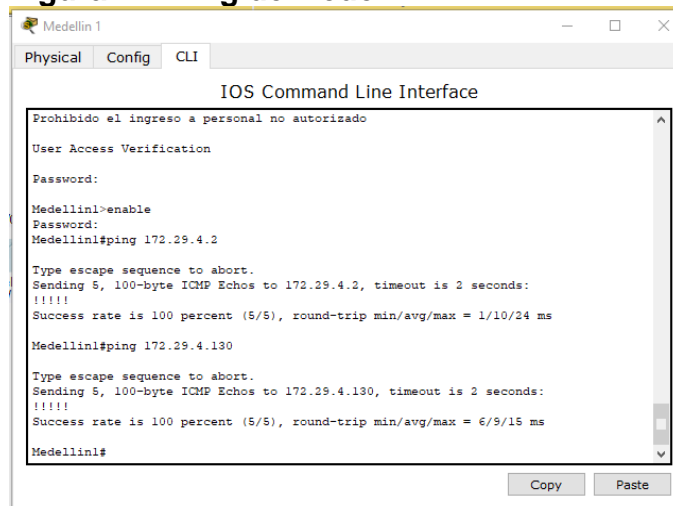
```

Password:
ISP>enable
Password:
ISP#configure t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.255.0 209.17.220.1
ISP(config)#ip route 172.29.0.0 255.255.255.0 209.17.220.5
ISP(config)#

```

Ping de Medellín 1 al PC-50 host y PC-40 host

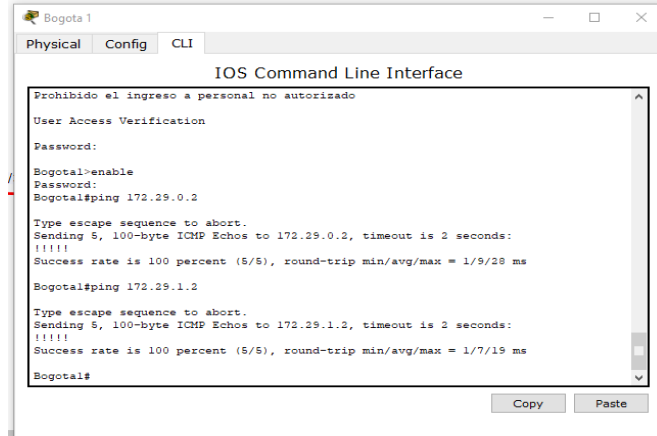
**Figura 11. Ping de Medellín1**



Ping de Bogotá 1 al PC-150 host y PC-200 host

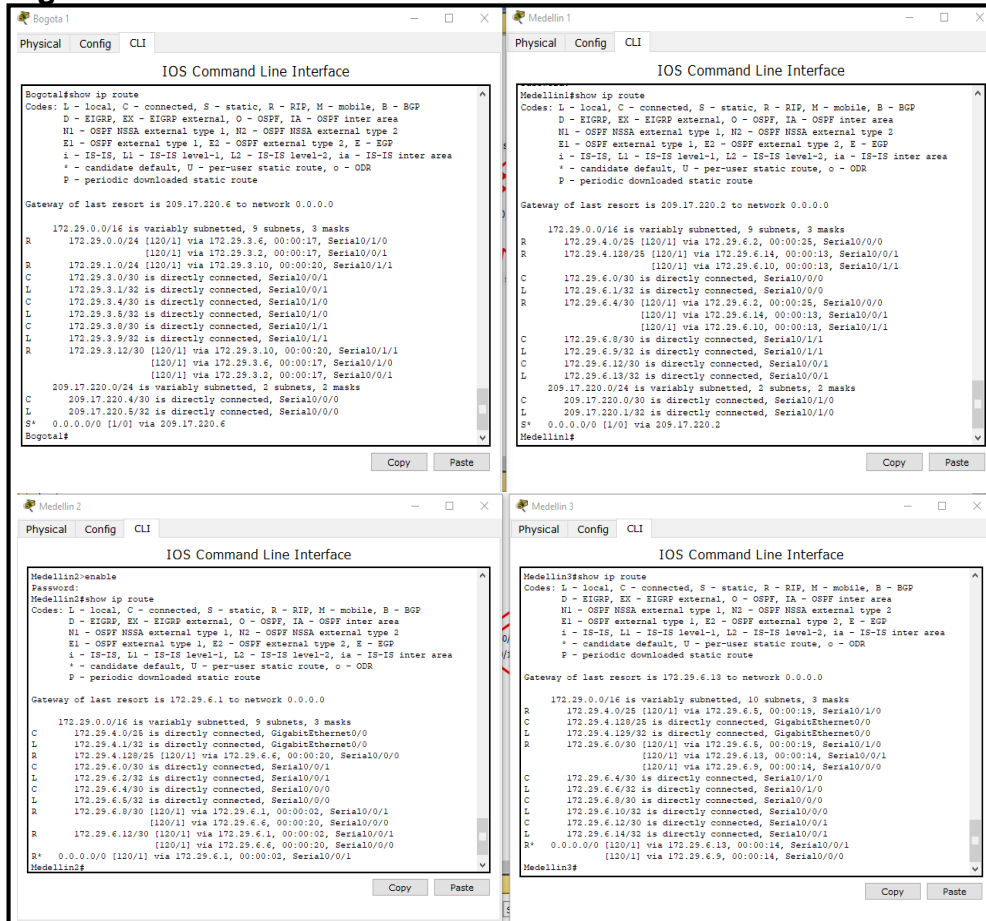


Figura 12. Ping de Bogota1

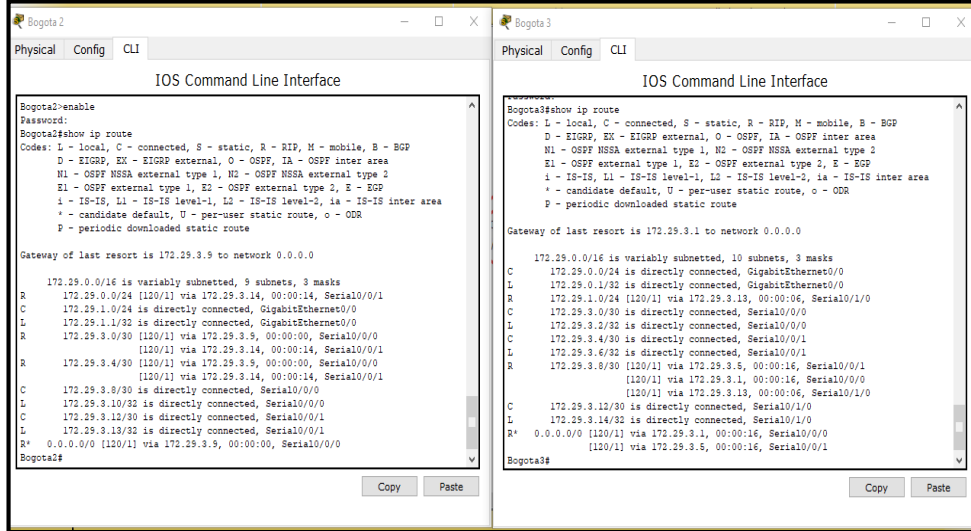


6. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Figura 13. Verificar tabla de enrutamiento en los Router



**Figura 13. Verificar tabla de enrutamiento en los Router**



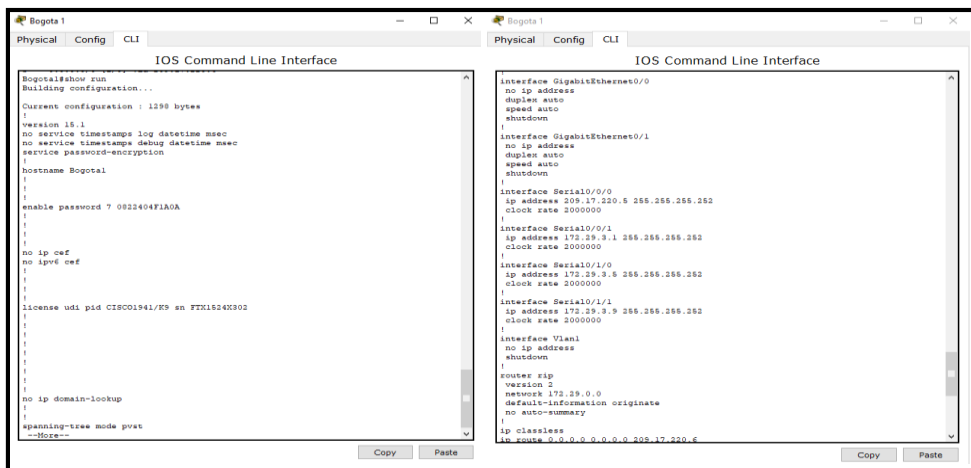
7. Verificar el balanceo de carga que presentan los routers.

8. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

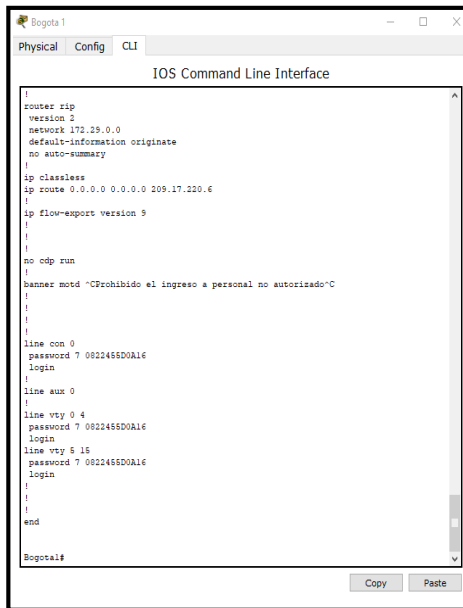
9. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante RIP.

10. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas

**Figura 14. Comando Show run para Bogota1**

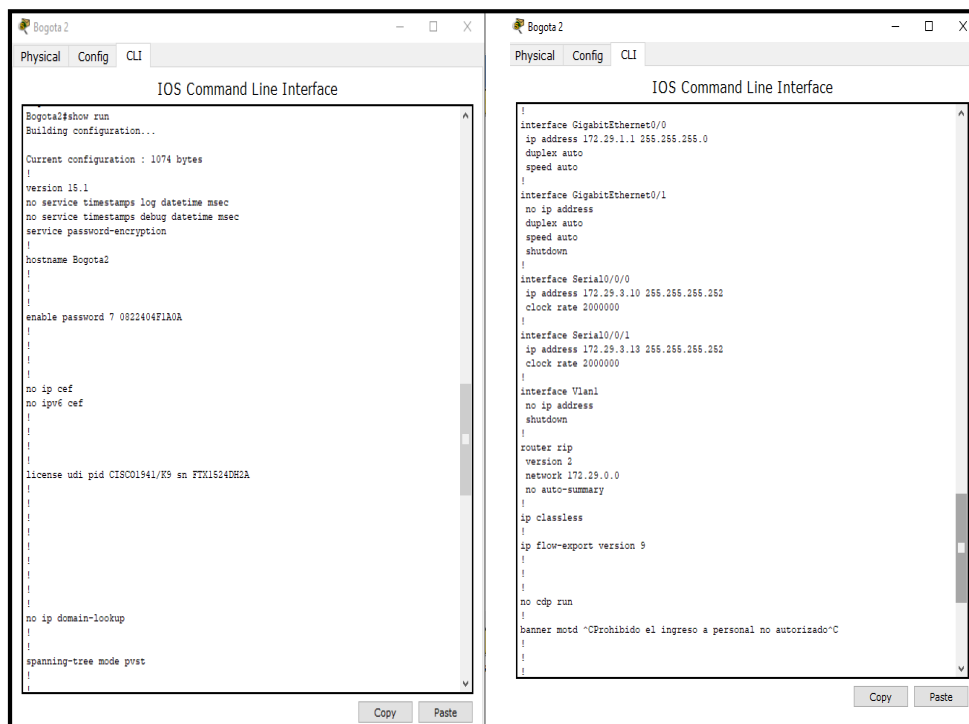


**Figura 14. Comando Show run para Bogota1**



```
!
router rip
version 2
network 172.29.0.0
default-information originate
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.6
!
ip flow-export version 5
!
!
no cdp run
!
banner motd ~CProhibido el ingreso a personal no autorizado~C
!
!
!
line con 0
password 7 0822465D0A16
login
!
line aux 0
!
!
line vty 0 4
password 7 0822465D0A16
login
line vty 5 15
password 7 0822465D0A16
login
!
!
!
end
Bogota1#
```

**Figura 15. Comando Show run para Bogota2**



```
Bogota2#show run
Building configuration...

Current configuration : 1074 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Bogota2
!
!
enable password 7 0822404F1A0A
!
!
!
no ip cef
no ipv6 cef
!
!
!
license udi pid CISC01941/R9 sn FTK16240H2A
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
```

```
!
interface GigabitEthernet0/0
ip address 172.29.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 172.29.3.10 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
ip address 172.29.3.13 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 172.29.0.0
no auto-summary
!
ip classless
!
ip flow-export version 5
!
!
!
no cdp run
!
banner motd ~CProhibido el ingreso a personal no autorizado~C
!
!
!
```

The screenshot shows a terminal window titled "Bogota2" with a menu bar containing "Physical", "Config", and "CLI". The main title of the session is "IOS Command Line Interface". The terminal displays a series of configuration commands entered by the user, each followed by a confirmation prompt. The commands are: "no ip address", "shutdown", "router rip", "version 2", "network 172.29.0.0", "no auto-summary", "ip classless", "ip flow-export version 9", "no cdp run", "banner motd ~CProhibido el ingreso a personal no autorizado~C", "line con 0", "password 7 0822455D0A16", "login", "line aux 0", "line vty 0 4", "password 7 0822455D0A16", "login", "line vty 5 15", "password 7 0822455D0A16", "login", and "end". The session concludes with the prompt "Bogota2#" appearing twice.

```
Bogota2
Physical Config CLI

IOS Command Line Interface

no ip address
shutdown
!
router rip
version 2
network 172.29.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
no cdp run
!
banner motd ~CProhibido el ingreso a personal no autorizado~C
!
!
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
!
!
!
end

Bogota2#
Bogota2#
```

The image displays two side-by-side screenshots of the IOS Command Line Interface (CLI) for a Cisco router named Medellin1. The left window shows the initial configuration steps, including setting the hostname, enabling passwords, and configuring the license. The right window shows the configuration of interfaces, including GigabitEthernet0/0, Serial0/0/0, Serial0/0/1, Serial0/1/0, Serial0/1/1, and Vlan1, along with router settings like RIP and classless IP routing.

```

Medellin1#show run
Building configuration...

Current configuration : 1301 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Medellin1
!
!
!
enable password 7 0822404F1A0A
!
!
!
no ip cef
no ipv6 cef
!
!
!
license udi pid CISCO1541/K9 sn FTK16241GSS
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!

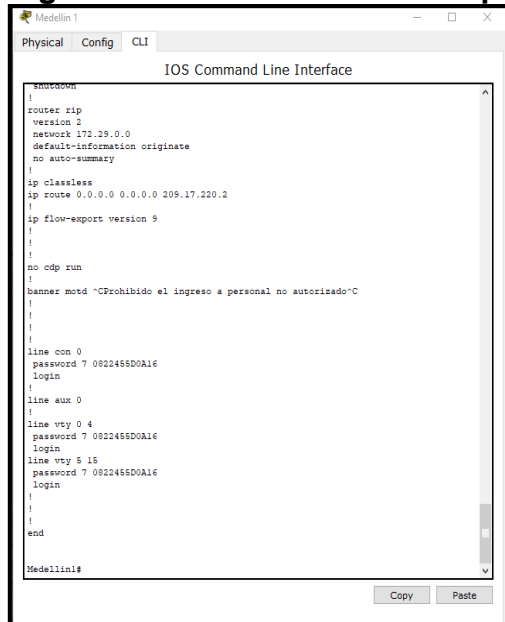
```

```

!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 172.29.6.1 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
ip address 172.29.6.13 255.255.255.252
clock rate 2000000
!
interface Serial0/1/0
ip address 209.17.220.1 255.255.255.252
clock rate 2000000
!
interface Serial0/1/1
ip address 172.29.6.9 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 172.29.0.0
default-information originate
no auto-summary
!
ip classless
ip source 0.0.0.0 0.0.0.0 209.17.220.2

```

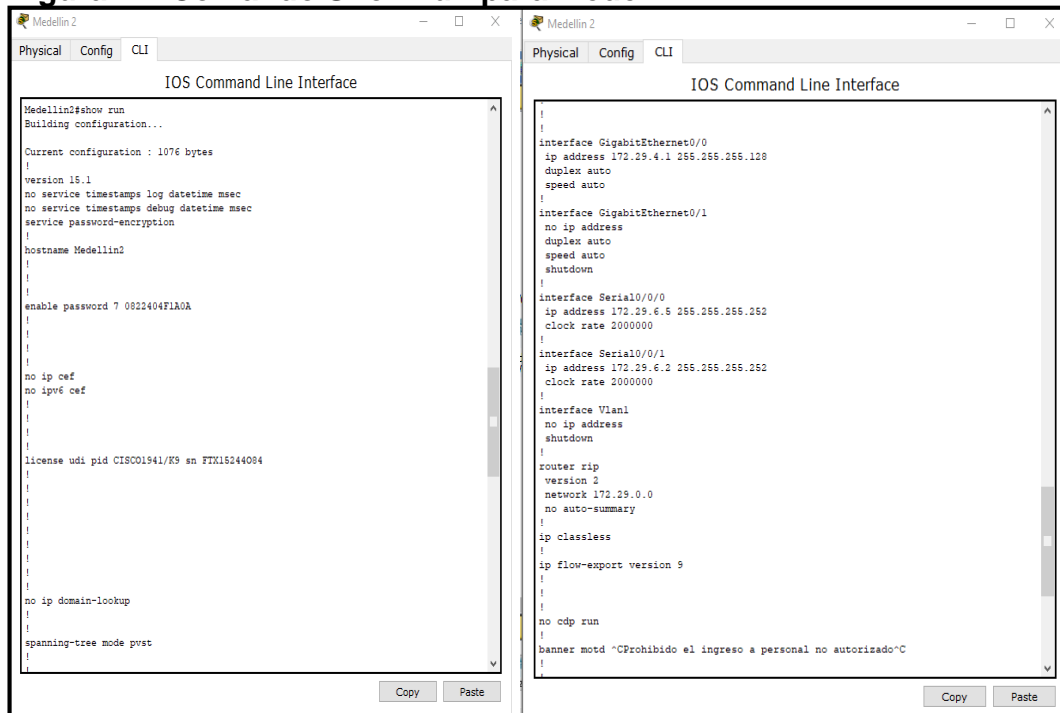
**Figura 16. Comando Show run para Medellin1**



```

Medellin1#
!
router rip
version 2
network 172.29.0.0
default-information originate
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.320.2
!
ip flow-export version 9
!
!
no cdp run
!
banner motd ^CProhibido el ingreso a personal no autorizado^C
!
!
!
line con 0
password 7 0822465D0A16
login
!
line aux 0
!
!
line vty 0 4
password 7 0822465D0A16
login
line vty 5 15
password 7 0822465D0A16
login
!
!
end
Medellin1#
  
```

**Figura 17. Comando Show run para Medellin2**



```

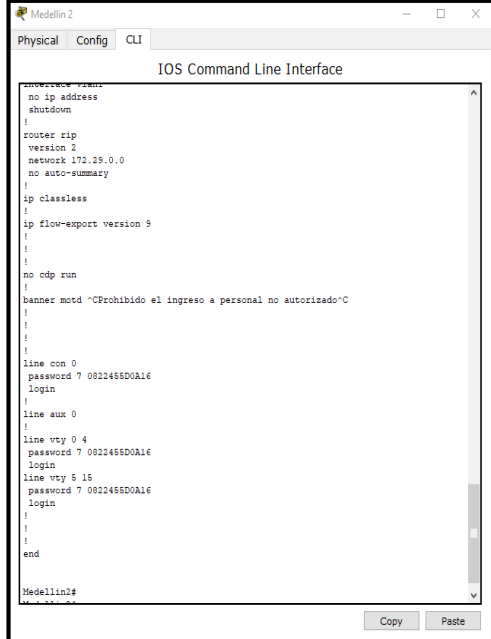
Medellin2#show run
Building configuration...

Current configuration : 1076 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Medellin2
!
!
enable password 7 0822404F1A0A
!
!
no ip cef
no ipv6 cef
!
!
!
license udi pid CISCO1941/K9 sn FTK15244084
!
!
!
no ip domain-lookup
!
spanning-tree mode pvst
!
!
  
```

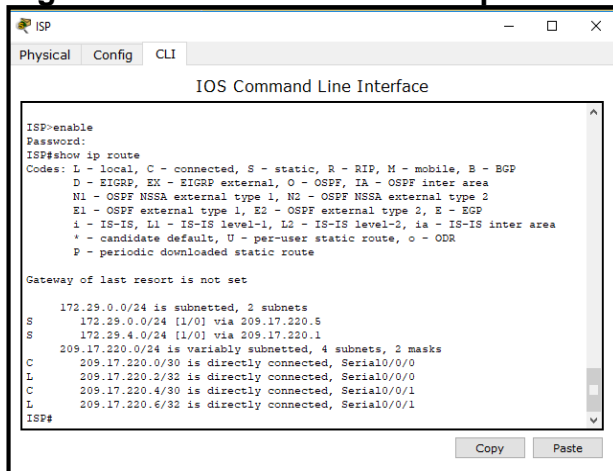
```

!
interface GigabitEthernet0/0
ip address 172.29.4.1 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 172.29.6.5 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
ip address 172.29.6.2 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 172.29.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
no cdp run
!
banner motd ^CProhibido el ingreso a personal no autorizado^C
!
!
  
```

**Figura 17. Comando Show run para Medellin2**



**Figura 18. Comando Show run para ISP**



11. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación entre otros datos.

## Router Bogotá 1

Bogota1>enable

Password:

Bogota1#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Bogota1(config)#router rip

Bogota1(config-router)#version 2

Bogota1(config-router)#do show ip route connected

C 172.29.3.0/30 is directly connected, Serial0/0/1

C 172.29.3.4/30 is directly connected, Serial0/1/0

C 172.29.3.8/30 is directly connected, Serial0/1/1

C 209.17.220.4/30 is directly connected, Serial0/0/0

Bogota1(config-router)#passive-interface s0/0/0

Bogota1(config-router)#

### **Router Medellín 1**

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

Medellin1>enable

Password:

Medellin1#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Medellin1(config)#router rip

Medellin1(config-router)#version 2

Medellin1(config-router)#do show ip route connected

C 172.29.6.0/30 is directly connected, Serial0/0/0

C 172.29.6.8/30 is directly connected, Serial0/1/1

C 172.29.6.12/30 is directly connected, Serial0/0/1

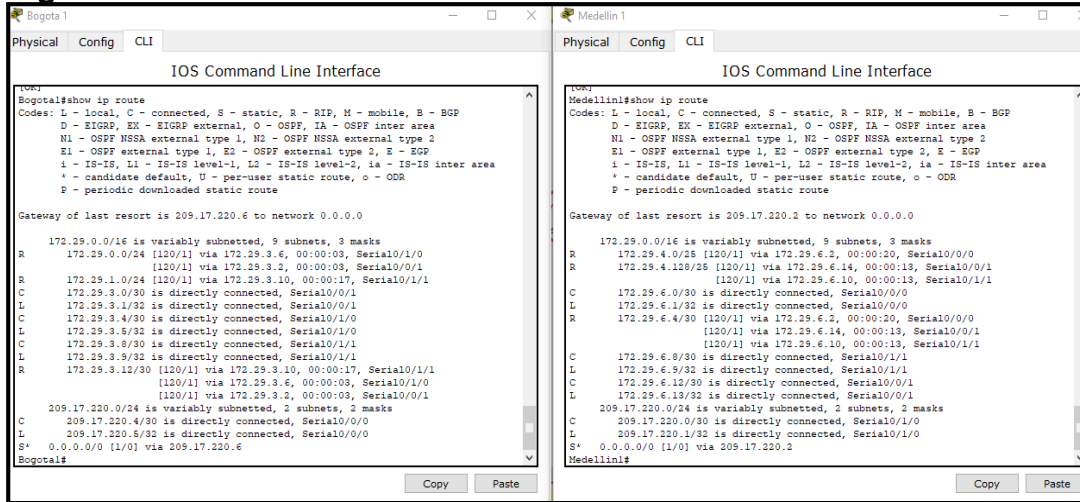
C 209.17.220.0/30 is directly connected, Serial0/1/0

Medellin1(config-router)#passive-interface s0/1/0

Medellin1(config-router)#

- 12.** Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

**Figura 19. Verificar la base de datos de RIP**



**13.** Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

## Router ISP

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

ISP>enable

Password:

ISP#configure t

Enter configuration commands, one per line. End with CNTL/Z.

ISP(config)#username Medellin1 password unad

ISP(config)#interface s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication pap

ISP(config-if)#ppp pap sent-username ISP password unad

ISP(config-if)#

## Router Medellín 1

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

Medellin1>enable

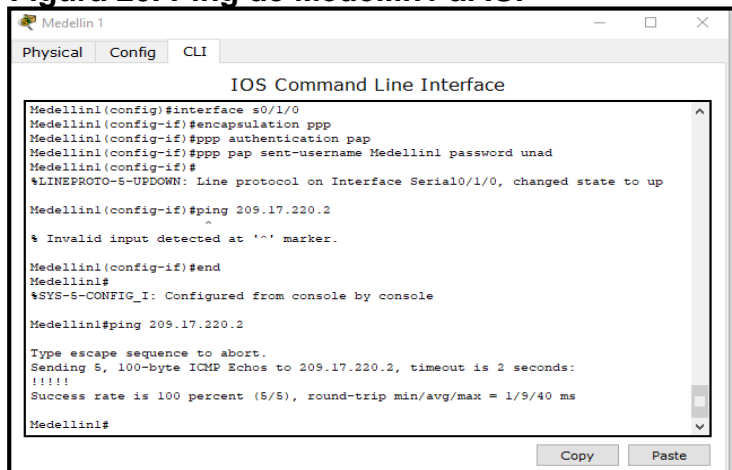


```

Password:
Medellin1#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state
to down
Medellin1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#username ISP password unad
Medellin1(config)#interface s0/1/0
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin1 password unad
Medellin1(config-if)#

```

**Figura 20. Ping de Medellin1 al ISP**



**14.** El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

## Router ISP

```

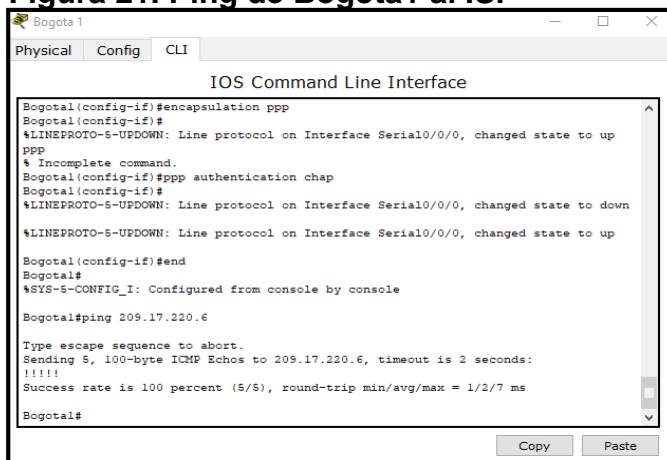
ISP#configure t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#username Bogota1 password unad
ISP(config)#interface s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to down
ISP(config-if)#ppp authentication chap
ISP(config-if)#

```

## Router Bogotá 1

```
Bogota1>enable
Password:
Bogota1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#username ISP password unad
Bogota1(config)#interface s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
ppp
% Incomplete command.
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Bogota1(config-if)#
```

**Figura 21. Ping de Bogota1 al ISP**



15. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

## Router Medellín 2

```

Medellin2>enable
Password:
Medellin2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.139
Medellin2(config)#ip dhcp pool medellin2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#dns-server 9.9.9.9
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool medellin3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#dns-server 9.9.9.9
Medellin2(dhcp-config)#exit
Medellin2(config)#

```

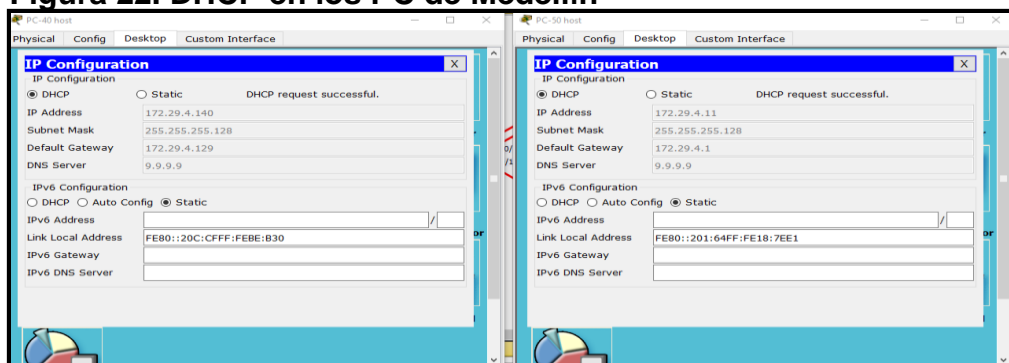
16. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

```

Prohibido el ingreso a personal no autorizado
User Access Verification
Password:
Medellin3>enable
Password:
Medellin3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#interface g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#

```

**Figura 22. DHCP en los PC de Medellín**



17. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes Lan.

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

Bogota2>enable

Password:

Bogota2#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10

Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10

Bogota2(config)#ip dhcp pool bogota2

Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0

Bogota2(dhcp-config)#default-router 172.29.1.1

Bogota2(dhcp-config)#dns-server 1.1.1.1

Bogota2(dhcp-config)#exit

Bogota2(config)#ip dhcp pool bogota3

Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0

Bogota2(dhcp-config)#default-router 172.29.0.1

Bogota2(dhcp-config)#dns-server 1.1.1.1

Bogota2(dhcp-config)#

18. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Bogota3#configure t

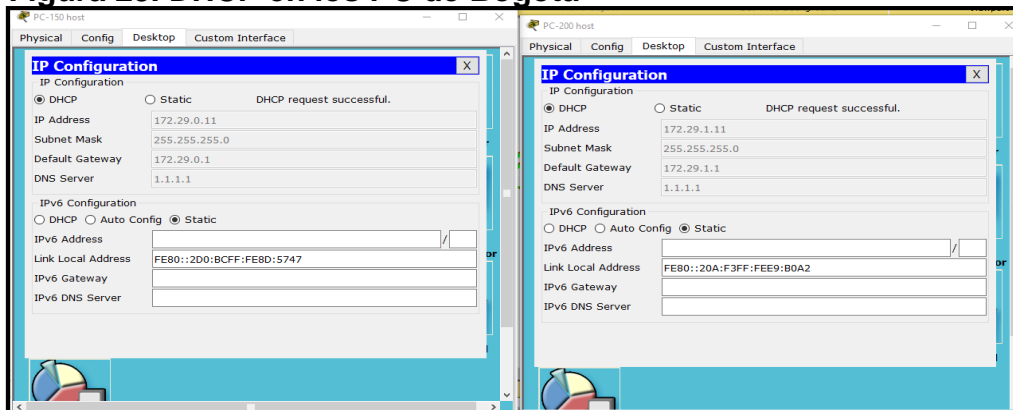
Enter configuration commands, one per line. End with CNTL/Z.

Bogota3(config)#interface g0/0

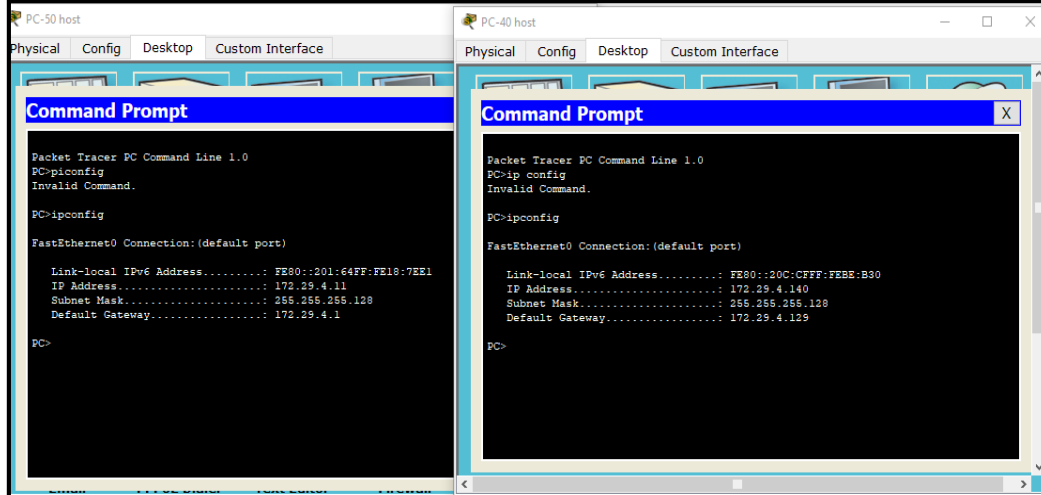
Bogota3(config-if)#ip helper-address 172.29.1.1

Bogota3(config-if)#

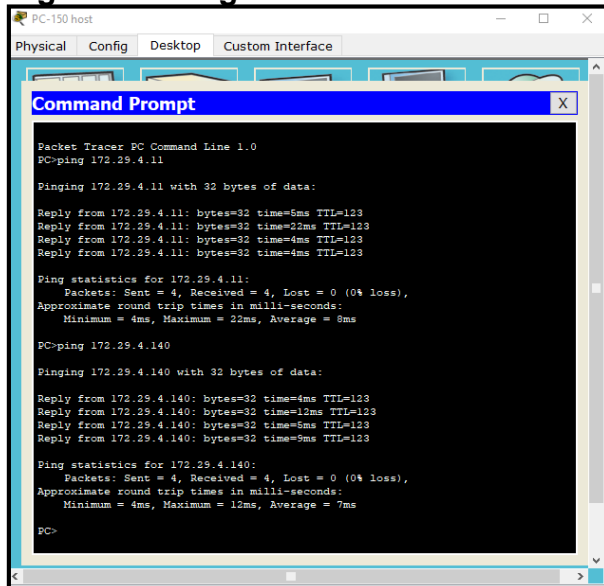
**Figura 23. DHCP en los PC de Bogotá**



**Figura 24. Verificar IP con el comando ipconfig**



**Figura 25. Ping de PC-150 a las demás PC**



19. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
20. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección

debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

```
Prohibido el ingreso a personal no autorizado
User Access Verification
Password:
Medellin1>enable
Password:
Medellin1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload
Medellin1(config)#access-list 1 permit
% Incomplete command.
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config)#interface s0/1/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#interface s0/0/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#interface s0/1/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#interface s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#
```

- 21.** Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

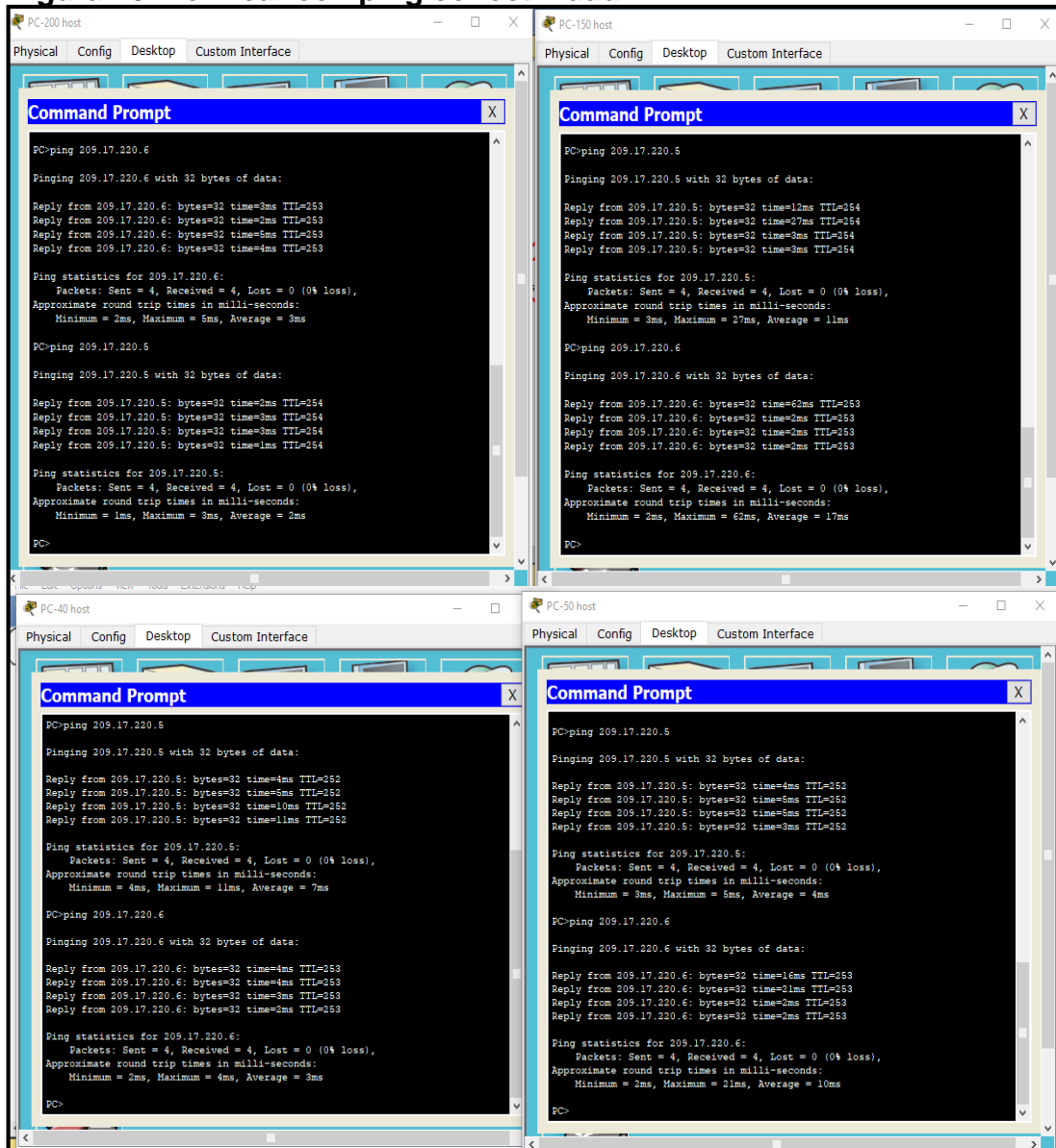
```
Prohibido el ingreso a personal no autorizado
User Access Verification
Password:
Bogota1>enable
Password:
Bogota1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip nat inside source list 1 interface s0/0/0 overload
Bogota1(config)#access-list 1 permit
% Incomplete command.
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota1(config)#interface s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#interface s0/0/1
Bogota1(config-if)#ip nat inside
```

```

Bogota1(config-if)#interface s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#interface s0/1/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#

```

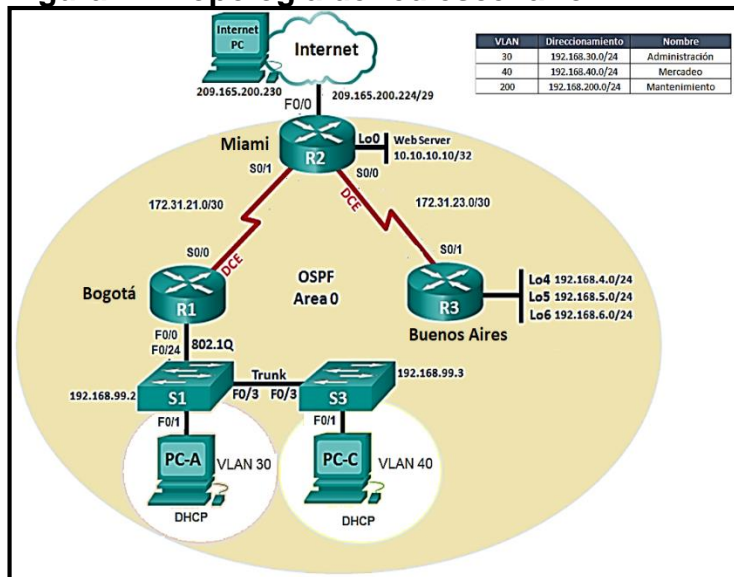
**Figura 26. Verificar con ping conectividad**



## 2. ESCENARIO 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red

**Figura 27. Topología de red escenario 2**



1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

**Tabla 2. Direccionamiento escenario 2**

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Gateway predeterminado
R1 (Bogotá)	S0/0/0 DCE	172.31.21.1	255.255.255.252	N/A
R2 (Miami)	S0/0/1	172.31.21.2	255.255.255.252	N/A
	S0/0/0 DCE	172.31.23.1	255.255.255.252	N/A
	F0/0	209.165.200.225	255.255.255.248	N/A
	F0/1	10.10.10.1	255.255.255.0	N/A
R3 (Buenos Aires)	S0/0/1	172.31.23.2	255.255.255.252	N/A



	Lo4	192.168.4.1	255.255.255.0	N/A
	Lo5	192.168.5.1	255.255.255.0	N/A
	Lo6	192.168.6.1	255.255.255.0	N/A
Internet PC	NIC	209.165.200.230	255.255.255.248	209.165.200.225
PC-A	NIC	DHCP	DHCP	DHCP
PC-C	NIC	DHCP	DHCP	DHCP
Web Server	NIC	10.10.10.10	255.255.255.0	10.10.10.1

2. Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

### Router Bogotá

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota
Bogota(config)#no ip domain-lookup
Bogota(config)#enable password class
Bogota(config)#line con 0
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#line vty 0 15
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#service password-encryption
Bogota(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Bogota(config)#end
Bogota#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#

```

### Router Miami

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.

```

```

Router(config)#hostname Miami
Miami(config)#no ip domain-lookup
Miami(config)#enable password class
Miami(config)#line con 0
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#exit
Miami(config)#line vty 0 15
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#exit
Miami(config)#service password-encryption
Miami(config)#banner motd "Prohibido el ingreso a personal no autorizado"
Miami(config)#end
Miami#
%SYS-5-CONFIG_I: Configured from console by console
Miami#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Miami#

```

## **Router Buenos Aires**

```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BuenosAires
BuenosAires(config)#no ip domain-lookup
BuenosAires(config)#enable password class
BuenosAires(config)#line con 0
BuenosAires(config-line)#password cisco
BuenosAires(config-line)#login
BuenosAires(config-line)#exit
BuenosAires(config)#line vty 0 15
BuenosAires(config-line)#password cisco
BuenosAires(config-line)#login
BuenosAires(config-line)#exit
BuenosAires(config)#service password-encryption
BuenosAires(config)#banner motd "Prohibido el ingreso a personal no autorizado"
BuenosAires(config)#end
BuenosAires#
%SYS-5-CONFIG_I: Configured from console by console
BuenosAires#copy run start

```

Destination filename [startup-config]?  
Building configuration...  
[OK]  
BuenosAires#

### Switch 1

```
Switch>enable
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable password class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "Prohibido el ingreso a personal no autorizado"
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

### Switch 3

```
Switch>enable
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable password class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 15
```

```

S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd "Prohibido el ingreso a personal no autorizado"
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S3#

```

### 3. Configuración de direcciones IP.

#### **Router Bogotá**

```

Prohibido el ingreso a personal no autorizado
User Access Verification
Password:
Bogota>enable
Password:
Bogota#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#interface s0/0/0
Bogota(config-if)#description connection to Miami
Bogota(config-if)#ip address 172.31.21.1 255.255.255.252
Bogota(config-if)#clock rate 128000
Bogota(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Bogota(config-if)#exit
Bogota(config)#ip route 0.0.0.0 0.0.0.0 172.31.21.2
Bogota(config)#exit
Bogota#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#

```

#### **Router Miami**

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

Miami>enable

Password:

Miami#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Miami(config)#interface s0/0/1

Miami(config-if)#description connection to Bogota

Miami(config-if)#ip address 172.31.21.2 255.255.255.252

Miami(config-if)#no shutdown

Miami(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Miami(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Miami(config-if)#interface s0/0/0

Miami(config-if)#description connection to BuenosAires

Miami(config-if)#ip address 172.31.23.1 255.255.255.252

Miami(config-if)#clock rate 128000

Miami(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Miami(config-if)#interface f0/0

Miami(config-if)#ip address 209.165.200.225 255.255.255.248

Miami(config-if)#no shutdown

Miami(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Miami(config-if)#interface f0/1

Miami(config-if)#description connection to Web Server

Miami(config-if)#ip address 10.10.10.1 255.255.255.0

Miami(config-if)#no shutdown

Miami(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Miami(config-if)#end

Miami#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

Miami#

## **Router Buenos aires**

Prohibido el ingreso a personal no autorizado

User Access Verification

Password:

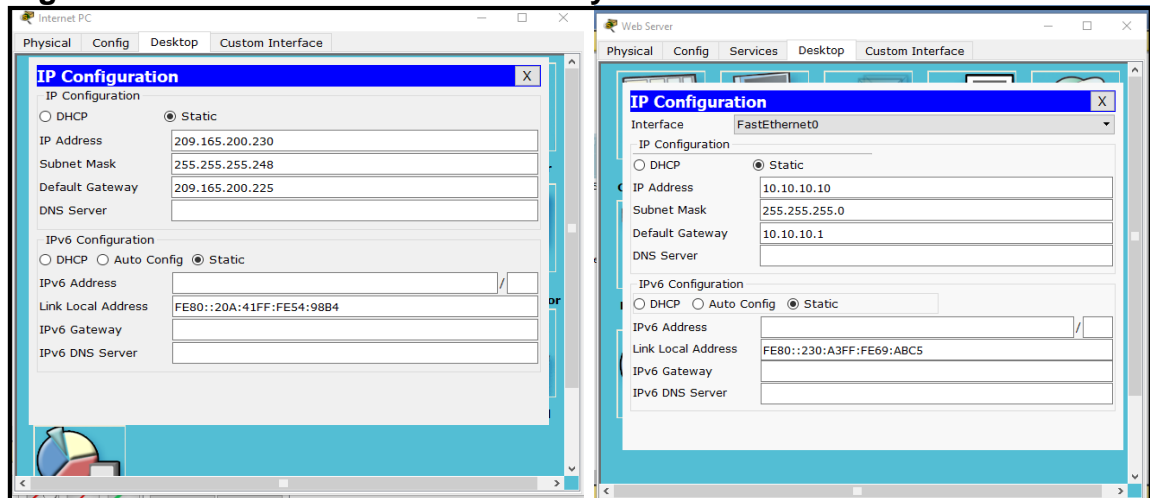
```

BuenosAires>enable
Password:
BuenosAires#configure t
Enter configuration commands, one per line. End with CNTL/Z.
BuenosAires(config)#interface s0/0/1
BuenosAires(config-if)#description conexion Miami
BuenosAires(config-if)#ip address 172.31.23.2 255.255.255.252
BuenosAires(config-if)#no shutdown
BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
BuenosAires(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
BuenosAires(config-if)#interface lo4
BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state
to up
BuenosAires(config-if)#exit
BuenosAires(config)#interface lo4
BuenosAires(config-if)#ip address 192.168.4.1 255.255.255.0
BuenosAires(config-if)#exit
BuenosAires(config)#interface lo5
BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state
to up
BuenosAires(config-if)#ip address 192.168.5.1 255.255.255.0
BuenosAires(config-if)#no shutdown
BuenosAires(config-if)#exit
BuenosAires(config)#interface lo6
BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state
to up
BuenosAires(config-if)#ip address 192.168.6.1 255.255.255.0
BuenosAires(config-if)#no shutdown
BuenosAires(config-if)#exit
BuenosAires(config)#interface lo4
BuenosAires(config-if)#no shutdown
BuenosAires(config-if)#exit
BuenosAires(config)#ip route 0.0.0.0 0.0.0.0 172.31.23.1
BuenosAires(config)#exit
BuenosAires#
%SYS-5-CONFIG_I: Configured from console by console

```

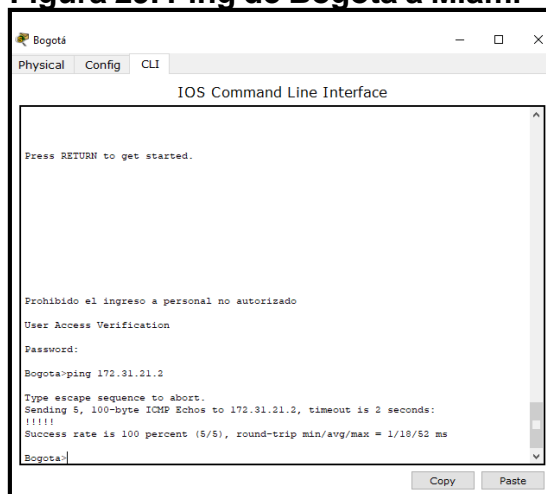
BuenosAires#copy run start  
 Destination filename [startup-config]?  
 Building configuration...  
 [OK]  
 BuenosAires#

**Figura 28. Dirección IP de Internet PC y Web Server**

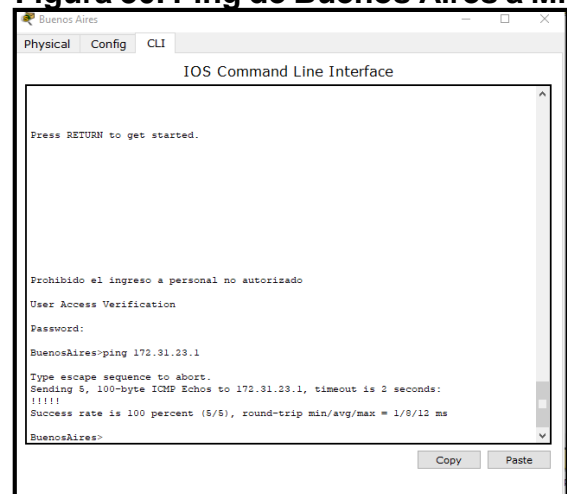


#### 4. Verificación entre routers

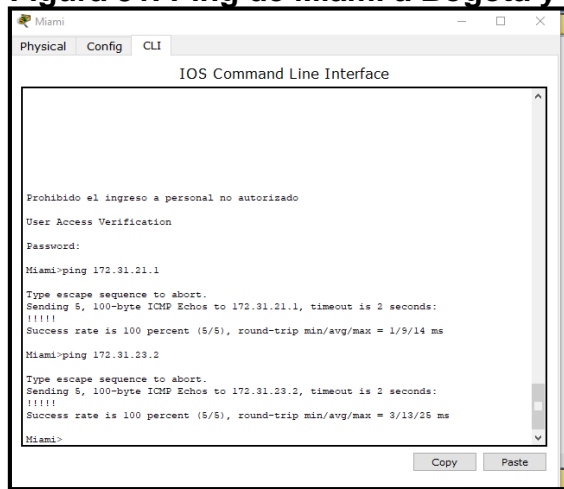
**Figura 29. Ping de Bogotá a Miami**



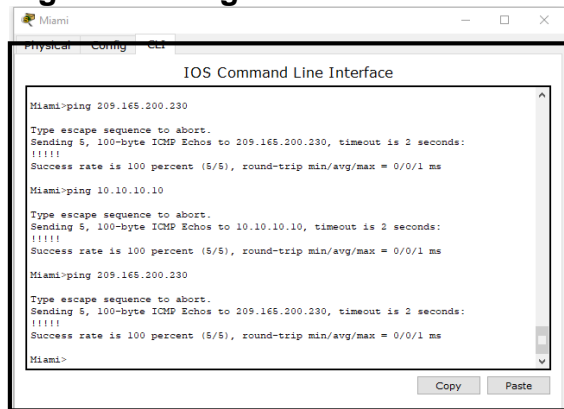
**Figura 30. Ping de Buenos Aires a Miami**



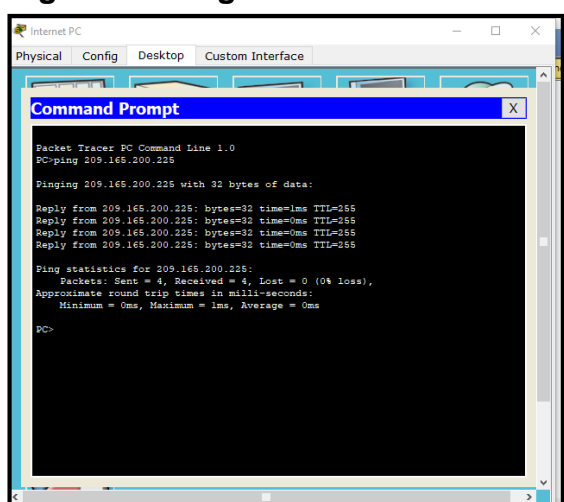
**Figura 31. Ping de Miami a Bogotá y Buenos Aires**



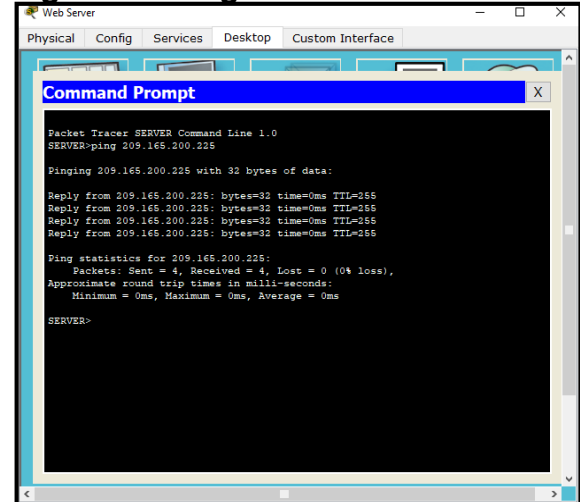
**Figura 32. Ping de Miami a Internet PC y Web Server**



**Figura 33. Ping de Internet PC a Miami**



**Figura 34. Ping de Web Server a Miami**





5. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

**Tabla 3. OSPFv2 area 0**

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

### Router Bogotá

```

Bogota#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router ospf 1
Bogota(config-router)#router-id 1.1.1.1
Bogota(config-router)#network 172.31.21.0 0.0.0.3 area 0
Bogota(config-router)#network 192.168.30.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.40.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.200.0 0.0.0.255 area 0
Bogota(config-router)#passive-interface fa0/0.30
Bogota(config-router)#passive-interface fa0/0.40
Bogota(config-router)#passive-interface fa0/0.200
Bogota(config-router)#exit
Bogota(config)#interface s0/0/0
Bogota(config-if)#bandwidth 256
Bogota(config-if)#exit
Bogota(config)#interface s0/0/0
Bogota(config-if)#ip ospf cost 9500
Bogota(config-if)#end
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
Bogota#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#

```

## Router Miami

User Access Verification

Password:

Miami>enable

Password:

Miami#configure t

Enter configuration commands, one per line. End with CNTL/Z.

Miami(config)#router ospf 1

Miami(config-router)#router-id 5.5.5.5

Miami(config-router)#network 172.31.21.0 0.0.0.3 area 0

Miami(config-router)#network 172.31.23.0 0.0.0.3 area 0

00:22:28: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from  
LOADING to FULL, Loading Done

Miami(config-router)#network 172.31.23.0 0.0.0.3 area 0

Miami(config-router)#network 10.10.10.0 0.0.0.255 area 0

Miami(config-router)#passive-interface fa0/0

Miami(config-router)#exit

Miami(config)#interface s0/0/1

Miami(config-if)#bandwidth 256

Miami(config-if)#exit

Miami(config)#interface s0/0/0

Miami(config-if)#bandwidth 256

Miami(config-if)#exit

Miami(config)#interface s0/0/0

Miami(config-if)#ip ospf cost 9500

Miami(config-if)#exit

Miami(config)#

## Router Buenos Aires

BuenosAires#configure t

Enter configuration commands, one per line. End with CNTL/Z.

BuenosAires(config)#router ospf 1

BuenosAires(config-router)#router-id 8.8.8.8

BuenosAires(config-router)#network 172.31.23.0 0.0.0.3 area 0

BuenosAires(config-router)#

00:27:14: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from  
LOADING to FULL, Loading Done

BuenosAires(config-router)#network 192.168.4.0 0.0.3.255 area 0

BuenosAires(config-router)#passive-interface lo4

BuenosAires(config-router)#passive-interface lo5

BuenosAires(config-router)#passive-interface lo6

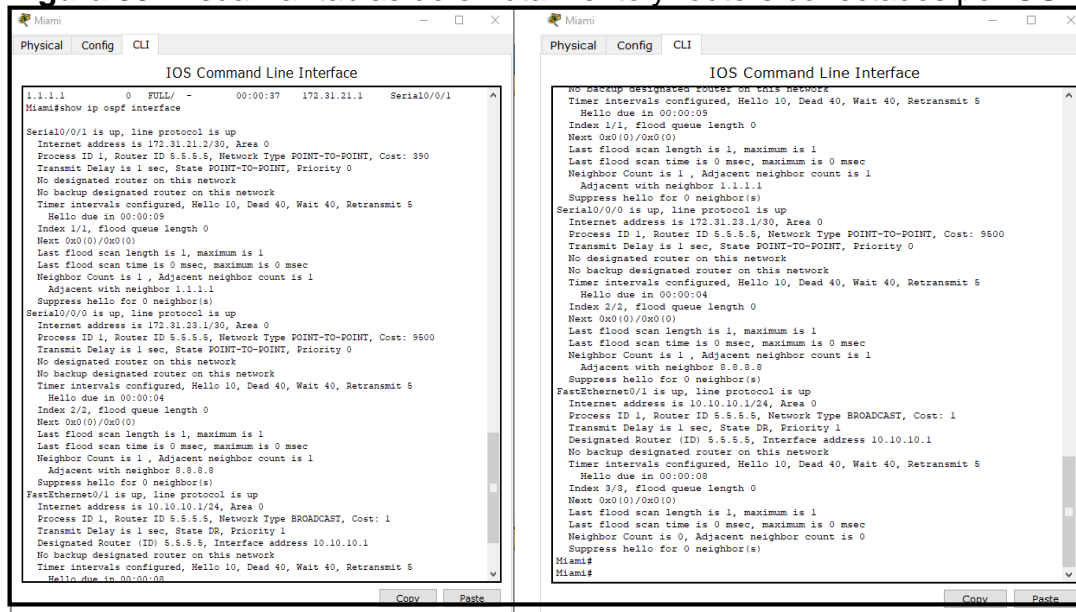
BuenosAires(config-router)#exit

```

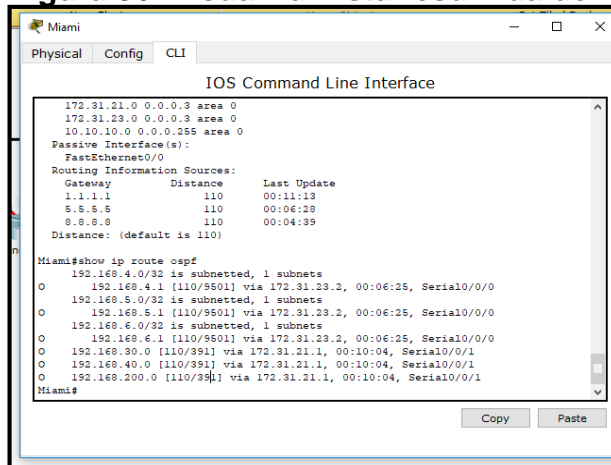
BuenosAires(config)#interface s0/0/1
BuenosAires(config-if)#bandwidth 256
BuenosAires(config-if)#end
BuenosAires#
%SYS-5-CONFIG_I: Configured from console by console
BuenosAires#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
BuenosAires#

```

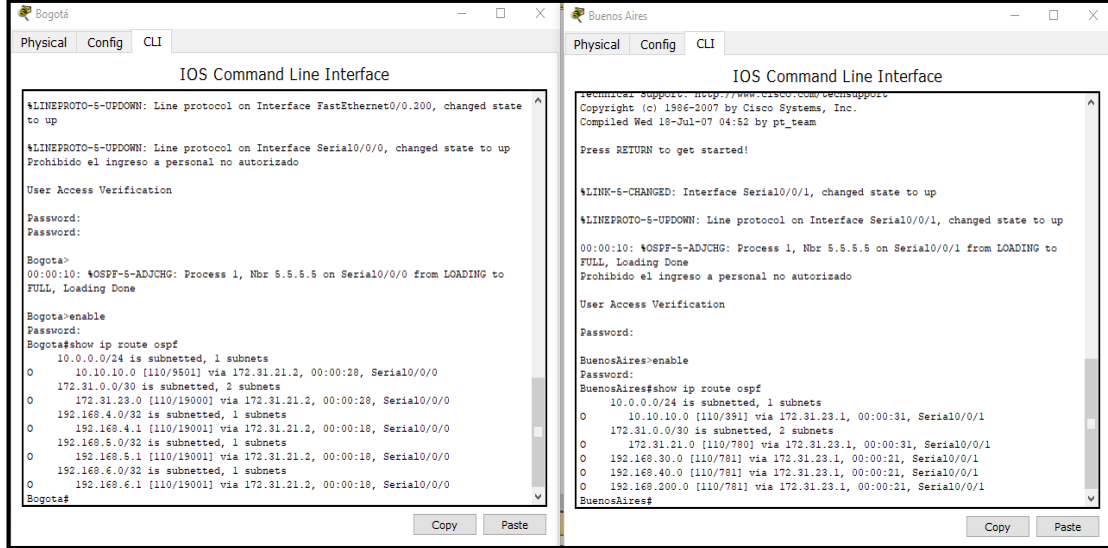
**Figura 35. Visualizar tablas de enrutamiento y routers conectados por OSPFv2**



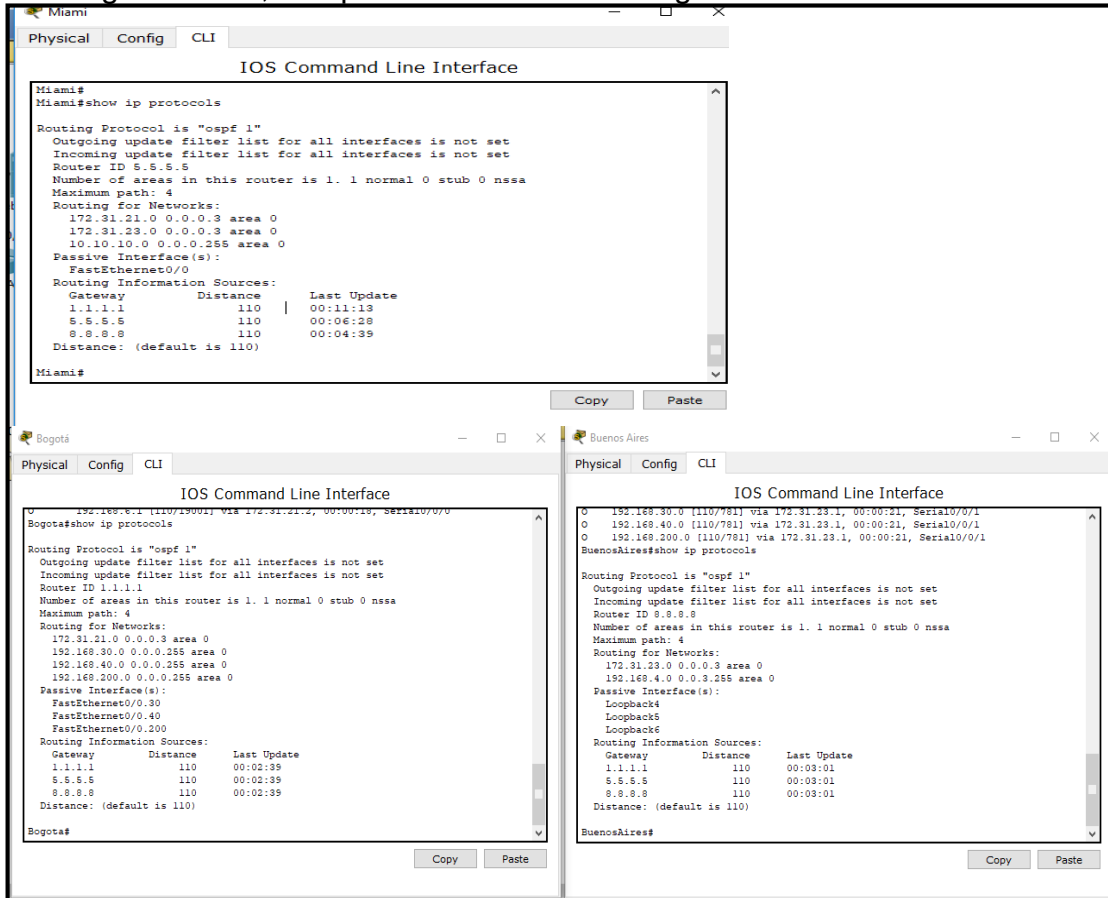
**Figura 36. Visualizar lista resumida de interfaces por OSPF**



**Figura 36. Visualizar lista resumida de interfaces por OSPF**



**Figura 37. Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.**



6. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

## **Switch 1**

### Configurar VLANs

```
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
```

### Puertos troncales

```
S1(config)#interface fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to
up
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface fa0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

### Puertos de acceso

```
S1(config-if)#interface range fa0/1-2, fa0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

### Encapsulamiento

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#exit
```

### Switch 3

#### Configurar VLANs

```
S3>enable
Password:
S3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
```

#### Puertos troncales

```
S3(config)#interface fa0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
```

#### Puertos de acceso

```
S3(config-if)#interface range fa0/1-2, fa0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```

#### Encapsulamiento

```
S3(config)#interface fa0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
```

### Router Bogotá

#### Routing

#### User Access Verification

```
Password:
Bogota>enable
Password:
Bogota#configure t
Enter configuration commands, one per line. End with CNTL/Z.
```

```

Bogota(config)#interface fa0/0.30
Bogota(config-subif)#description Administracion LAN
Bogota(config-subif)#encapsulation dot1q 30
Bogota(config-subif)#ip address 192.168.30.1 255.255.255.0
Bogota(config-subif)#interface fa0/0.40
Bogota(config-subif)#description Mercadeo LAN
Bogota(config-subif)#encapsulation dot1q 40
Bogota(config-subif)#ip address 192.168.40.1 255.255.255.0
Bogota(config-subif)#interface fa0/0.200
Bogota(config-subif)#description Mantenimiento LAN
Bogota(config-subif)#encapsulation dot1q 200
Bogota(config-subif)#ip address 192.168.200.1 255.255.255.0
Bogota(config-subif)#end
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
Bogota#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#interface fa0/0
Bogota(config-if)#no shutdown
Bogota(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200,
changed state to up
Bogota(config-if)#end
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
Bogota#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#

```

## 7. En el Switch 3 deshabilitar DNS lookup

```
S3>enable
```

Password:

S3#configure t

Enter configuration commands, one per line. End with CNTL/Z.

S3(config)#no ip domain-lookup

S3(config)#

**8. Asignar direcciones IP a los Switches acorde a los lineamientos.**

### **Switch 1**

S1(config)#interface vlan 200

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

S1(config-if)#ip address 192.168.200.2 255.255.255.0

S1(config-if)#no shutdown

S1(config-if)#ip default-gateway 192.168.200.1

### **Switch 3**

S3(config)#interface vlan 200

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S3(config-if)#ip address 192.168.200.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#ip default-gateway 192.168.200.1

**9. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.**

### **Switch 1**

S1(config)#interface range fa0/2, fa0/4-23, g0/1-2

S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down



%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down  
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down  
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down  
S1(config-if-range)#

### Switch 3

```
S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S3(config-if-range)#
```

**10.** Implement DHCP and NAT for IPv4

**11.** Configurar R1 como servidor DHCP para las VLANs 30 y 40.

**12.** Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

**Tabla 4. Configurar DHCP pool**

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

**13.** Configurar NAT en R2 para permitir que los host puedan salir a internet

**14.** Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

**15.** Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

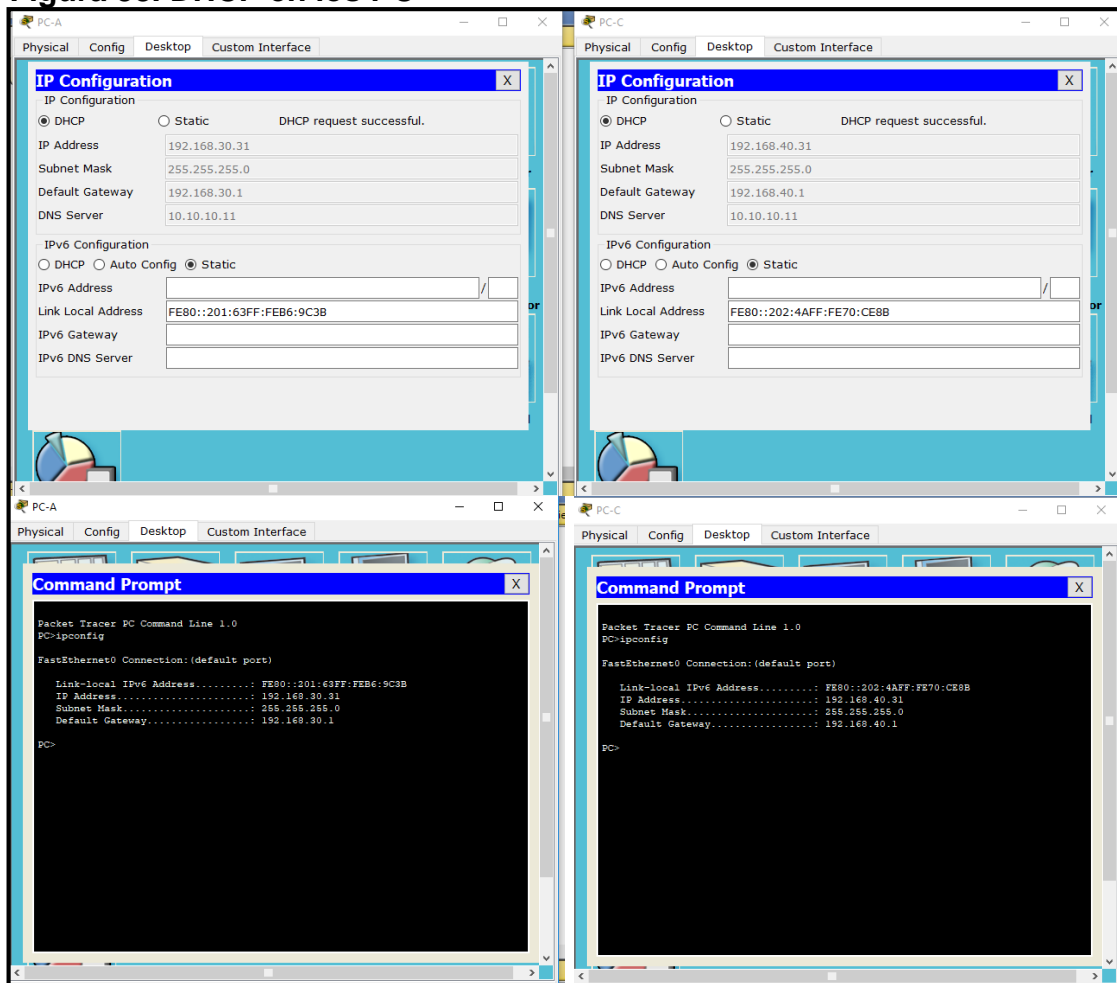
```
Bogota>enable
Password:
Bogota#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
Bogota(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
Bogota(config)#ip dhcp pool ADMINISTRACION
```

```

Bogota(dhcp-config)#dns-server 10.10.10.11
Bogota(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.
Bogota(dhcp-config)#default-router 192.168.30.1
Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0
Bogota(dhcp-config)#ip dhcp pool MERCADEO
Bogota(dhcp-config)#dns-server 10.10.10.11
Bogota(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.
Bogota(dhcp-config)#default-router 192.168.40.1
Bogota(dhcp-config)#network 192.168.40.0 255.255.255.0
Bogota(dhcp-config)#exit
Bogota(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Bogota(config)#interface fa0/0
Bogota(config-if)#ip nat outside
Bogota(config-if)#exit
Bogota(config)#interface fa0/1
Bogota(config-if)#ip nat inside
Bogota(config-if)#exit
Bogota(config)#access-list 1 permit 192.168.30.0 0.0.0.255
Bogota(config)#access-list 1 permit 192.168.40.0 0.0.0.255
Bogota(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Bogota(config)#ip nat pool CONECTAR 209.165.200.225 209.165.200.228
netmask 255.255.255.248
Bogota(config)#ip nat inside source list 1 pool CONECTAR
Bogota(config)#ip access-list standard ADMIN-CISCO
Bogota(config-std-nacl)#permit host 172.31.21.1
Bogota(config-std-nacl)#permit host 172.31.23.1
Bogota(config-std-nacl)#exit
Bogota(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
Bogota(config)#exit
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
Bogota#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#

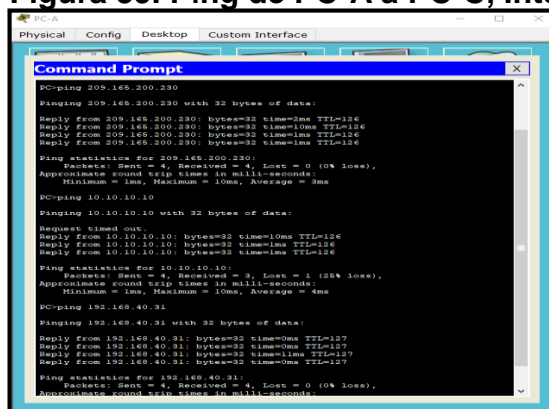
```

**Figura 38. DHCP en los PC**

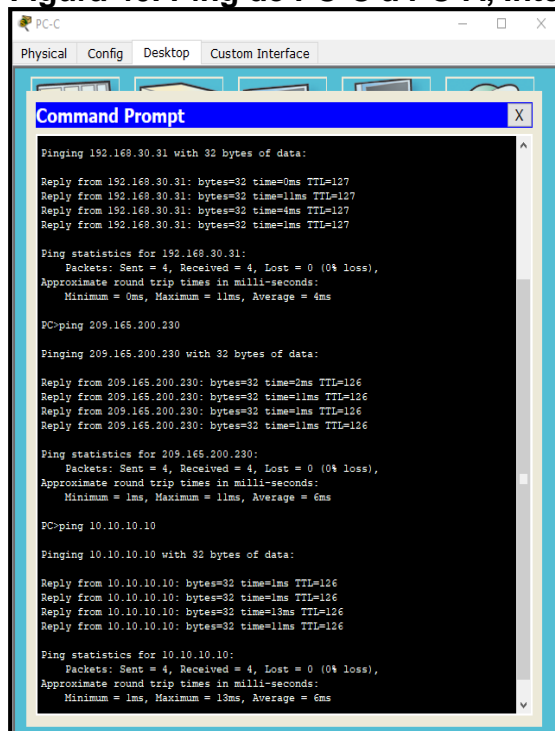


16. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute

**Figura 39. Píng de PC-A a PC-C, Internet PC y Web Server**



**Figura 40. Píng de PC-C a PC-A, Internet PC y Web Server**



```

PC-C
Physical Config Desktop Custom Interface

Command Prompt

Pinging 192.168.30.31 with 32 bytes of data:

Reply from 192.168.30.31: bytes=32 time=0ms TTL=127
Reply from 192.168.30.31: bytes=32 time=1ms TTL=127
Reply from 192.168.30.31: bytes=32 time=4ms TTL=127
Reply from 192.168.30.31: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 4ms

PC>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=2ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 6ms

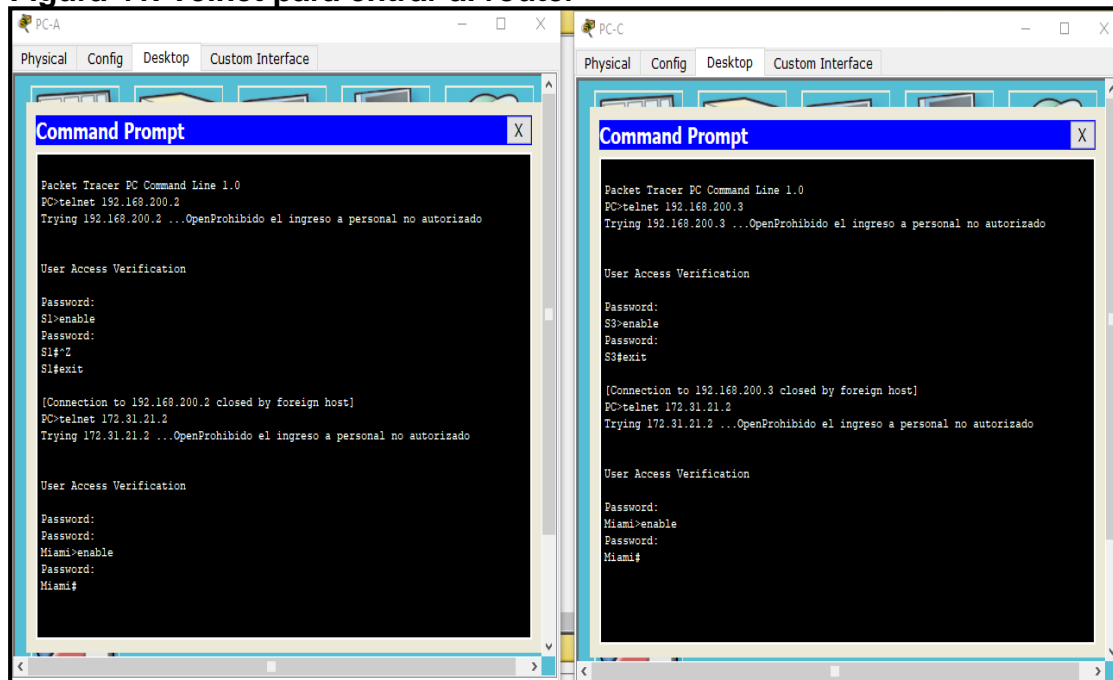
PC>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=1ms TTL=126
Reply from 10.10.10.10: bytes=32 time=1ms TTL=126
Reply from 10.10.10.10: bytes=32 time=13ms TTL=126
Reply from 10.10.10.10: bytes=32 time=1ms TTL=126

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 6ms
  
```

**Figura 41. Telnet para entrar al router**



```

PC-A
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>telnet 192.168.200.2
Trying 192.168.200.2 ...OpenProhibido el ingreso a personal no autorizado

User Access Verification

Password:
S1>enable
Password:
S1#~2
S1#exit

[Connection to 192.168.200.2 closed by foreign host]
PC>telnet 172.31.21.2
Trying 172.31.21.2 ...OpenProhibido el ingreso a personal no autorizado

User Access Verification

Password:
Miami>enable
Password:
Miami#
  
```

```

PC-C
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>telnet 192.168.200.3
Trying 192.168.200.3 ...OpenProhibido el ingreso a personal no autorizado

User Access Verification

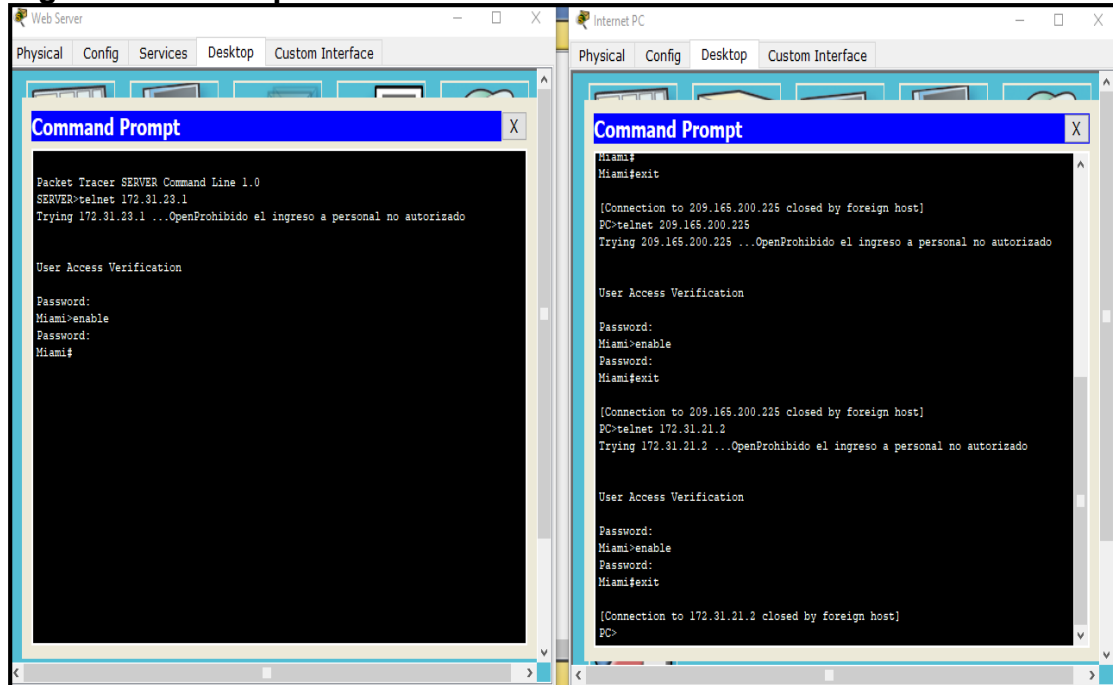
Password:
S3>enable
Password:
S3#exit

[Connection to 192.168.200.3 closed by foreign host]
PC>telnet 172.31.21.2
Trying 172.31.21.2 ...OpenProhibido el ingreso a personal no autorizado

User Access Verification

Password:
Miami>enable
Password:
Miami#
  
```

**Figura 41. Telnet para entrar al router**



## CONCLUSIÓN

Los equipos que se utilizarón en el diseño, configuración e instalaciones de redes, tienen diferentes características, que dependen en gran medida de los requerimientos del cliente, el cumplimiento regulatorio y el costo que se pueda asumir; entre estos dispositivos podemos encontrar switch y router, que soportan en gran medida la operación de las redes. Para el caso de los swicth permiten la conexión de múltiples dispositivos en la misma red, controlando el flujo de datos y dirigirlo. Para el caso de estos equipos en la marca CISCO, funcionan con un sistema operativo InternetWork (IOS) y no requieren configuraciones adicionales para su funcionamiento, pero permiten que se realicen configuraciones manuales que optimizan la velocidad, ancho de banda, seguridad, entre otros aspectos.

El IOS de CISCO, permite que los dispositivos establezcan las funciones básicas de enrutamiento y conmutación, el acceso y escalabilidad a los recursos de la red. Para el caso de los Switch estos puedan ser administrados remotamente, se requiere de la configuración de la dirección IP y un Gateway predeterminado, con lo cual se asegura su operación en la red.

Con el desarrollo del presente trabajo fue posible demostrar destrezas en cuanto a la configuración de equipos de red Cisco, como Routers y Switches

Se logró llevar a cabo de manera correcta la configuración de los switches, router así como también las características de seguridad de los mismos, la configuración de IPv4, la creación y configuración de VLANS, puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN, Routing, implementar DHCP y NAT para IPv4, por otro lado, configurar el enrutamiento de red usando el protocolo RIP versión 2 para redistribuirlo en las publicaciones RIP, las rutas estáticas dirigidas hacia cada red interna, deshabilitar la propagación RIP, encapsulamiento y autenticación PPP y configurar PAT.



## **BIBLIOGRAFÍA**

CISCO. (2014). Capítulo 1. Conceptos de routing. Recuperado de:  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1.0.1.1>

CISCO. (2014). Capítulo 2. Routing estático. Recuperado de  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2.0.1.1>

CISCO. (2014). Capítulo 3. Routing dinámico. Recuperado de  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3.0.1.1>

CISCO. (2014). Capítulo 4. Redes conmutadas. Recuperado de  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4.0.1.1>

CISCO. (2014). Capítulo 5. Configuración del switch. Recuperado de  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5.0.1.1>

CISCO. (2014). Capítulo 6. VLAN. Recuperado de:  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6.0.1.1>

CISCO. (2014). Capítulo 7. Listas de control de acceso. Recuperado de:  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7.0.1.1>

CISCO. (2014). Capítulo 8. DHCP. Recuperado de:  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8.0.1.1>

CISCO. (2014). Capítulo 9. NAT para IPv4. Recuperado de:  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9.0.1.1>

CISCO. (2014). Capítulo 10. Detección, administración y mantenimiento de dispositivos. Recuperado de:  
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10.0.1.1>